View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Digital Repository @ Iowa State University

IOWA STATE UNIVERSITY
Digital Repository

Retrospective Theses and Dissertations

Iowa State University Capstones, Theses and Dissertations

1996

Coding theory and discrete transforms

Feng-Luan Hsu
Iowa State University

Follow this and additional works at: https://lib.dr.iastate.edu/rtd

 Part of the Mathematics Commons

Recommended Citation

Hsu, Feng-Luan, "Coding theory and discrete transforms " (1996). *Retrospective Theses and Dissertations*. 11154.
https://lib.dr.iastate.edu/rtd/11154

This Dissertation is brought to you for free and open access by the Iowa State University Capstones, Theses and Dissertations at Iowa State University Digital Repository. It has been accepted for inclusion in Retrospective Theses and Dissertations by an authorized administrator of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.

INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI

A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor MI 48106-1346 USA
313/761-4700 800/521-0600

Coding theory and discrete transforms

by

Feng-Luan Hsu

A Dissertation Submitted to the

Graduate Faculty in Partial Fulfillment of the

Requirements for the Degree of

DOCTOR OF PHILOSOPHY

Department: Mathematics
Major: Mathematics

Approved:

Signature was redacted for privacy.

In Charge of Major Work

Signature was redacted for privacy.

For the Major Department

Signature was redacted for privacy.

For the Graduate College

Iowa State University
Ames, Iowa
1996

Copyright © Feng-Luan Hsu, 1996. All rights reserved.

UMI Number: 9626042

UMI Microform 9626042
Copyright 1996, by UMI Company. All rights reserved.

This microform edition is protected against unauthorized copying under Title 17, United States Code.

UMI
300 North Zeeb Road
Ann Arbor, MI 48103

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGMENTS

First of all, I would like to express my deepest gratitude to my major advisor, Professor Jonathan D. H. Smith, for suggesting me the problems and for his expert guidance throughout the preparation of this thesis. All through my graduate study at Iowa State University, he has been a constant resource of encouragements, inspiration, and tremendous ideas. Not only his way of problem-thinking and problem-solving that has benefited me most in research, but also his wisdom in life that has influenced me in every respect of life. It has been a great pleasure to work with such a scholar of knowledge, insight, and character.

I want to thank Professors Clifford Bergman, James Cornette, Herbert T. David, and Sung Yell Song for serving on my POS committee and giving their time and assistance during my studies at Iowa State University.

Special thanks are due to Professor Jack Lutz in the Department of Computer Science for sponsoring the use of the HP-UX machines in his department. It would have been difficult to obtain the graphical and tabular data presented here without the use of these machines.

I am also grateful to Ruth De Boer, Fran Hartman, Jan Nyhus, Ellen Olson, and Jim Lathrop for helping me in lots of different ways.

Most of all, I thank my parents, Jung-Hsin Hsu and A-Yen Tang Hsu, for their

never-ending love and support. Their encouragement and support make it possible for me to receive a higher education. I also thank my husband, Chih-Yao, for his patience, encouragement, assistance, and support; and my son Ian, for bringing me so much fun and joy. This dissertation is dedicated to them with my sincere appreciation.

CHAPTER 1. INTRODUCTION

The theory of error detecting and correcting codes is that branch of engineering and mathematics which deals with the reliable transmission and storage of data. The channels or the information media are not 100% reliable in practice, in the sense that *noise* (any form of interference) frequently causes data to be distorted.

To deal with this undesirable but inevitable situation, some form of *redundancy* is incorporated in the original data. With this redundancy, even if errors are introduced (up to some tolerance level), the original information can be recovered, or at least the presence of errors can be detected.

One of the problems to be resolved then is to determine how the channel encoder should add redundancy to the source encoder output. Another problem is to determine how the channel decoder should decide which sequence to decode to.

The design of error-correcting block codes has traditionally been influenced by two factors: an assumption of "white noise" (random noise) in the channel, and imposition of a severe limitation on the storage space available to the encoding and decoding algorithms. Under these influences, algebraic coding theory has been led to comprise an impressive directory of mathematically structured codes and their distance distributions. Nevertheless, in assessing the progress of the field a decade ago, Hamming [Ha, Chap 11.13] made the following comments:

> In the year 1985, we are seeing a great decrease in the cost of storage, and hence there is a need to reconsider all the theory that we have developed in the past. Methods of design, encoding, and decoding which depend more on table look up and other forms of storage and less on computing need to be researched and developed. Again, you need to be warned that the theory is almost all designed to meet white noise, and in practice often the noise is not white and the theoretical benefits of a code may therefore not be realized in practice.

The general loop transversal approach to the construction of linear block codes, introduced in [Sm], ultimately relies more on the availability of cheap storage than on the use of exceptional mathematical structures. Rather than focusing on the code itself as the primary object of interest, the approach (see [Sm]) to the construction of linear block codes concentrates on the set of errors corrected by the code. These errors do not necessarily have to form a ball, as they would under the assumption of white noise, but might equally well form an asymmetric figure corresponding to bursts or some other distribution.

The basis for the loop transversal approach is the observation that the set T of errors corrected by a linear code C in a channel V forms a *loop transversal* from V to C. Recall that a transversal T to a subgroup C of a group $(V,+,0)$ is a subset of V with $V = \dot{\bigcup}_{t\in T}(C+t)$. Thus each element x of V can be expressed uniquely as $x = x^\delta + x^\varepsilon$, with $x^\delta \in C$ and $x^\varepsilon \in T$. In the coding context, a received word x is assumed to have resulted from exposure to the error x^ε, and is thus decoded as x^δ.

Define a binary operation $*$ on T by $t * u = (t+u)^\varepsilon$. Then for any t, u in T, the equation $v * t = u$ has a unique solution v. If the equation $t * v = u$ also has a unique solution, then T is a *loop transversal.* Equivalently, the algebra $(T, *, 0_\varepsilon)$ is a loop.

If the channel V is a vector space over a field F, and the code C is a subspace of V, then is said to be a linear code. Define $\lambda \times t = (\lambda t)\varepsilon$ for x in F and t in T. We

then have that $(T, *, F)$ is a vector space over F, where T is the set of errors corrected by the code C. Knowledge of the vector space $(T, *, F)$ is sufficient to determine the code C by *local duality*, which says that for $t,\ u \in T,\ t + u + t * u \in C$. Also, note that $(x + y)\varepsilon = x\varepsilon * y\varepsilon$ and $(\lambda x)\varepsilon = \lambda \times (x\varepsilon)$ for λ in F and $x,\ y$ in V. Thus the *parity map* $\varepsilon : (V, +, F) \longrightarrow (T, *, F)$ is a linear transformation. Since the code is the kernel of the parity map, the matrices of ε with respect to appropriate bases are parity-check matrices.

To get $(T, *, F)$, we use an isomorphism $S : (T, *) \rightarrow (G, +)$, for example a monomorphism $S : (T, *) \rightarrow (\mathbf{N}, +_2)$ in binary case. Here $+_2$ is the nim-addition. We call the monomorphism $S : (T, *) \rightarrow (\mathbf{N}, +_2)$ a *syndrome function.* The paper [HmS] gives more detail of the general loop transversal approach to the construction of linear codes, focusing especially on the greedy loop transversal algorithm in the binary case.

In the paper entitled "Logarithms, Syndrome Functions, and the Information Rates of Greedy Loop Transversal Codes" (Chapter 2), we use a greedy algorithm to construct syndrome functions of binary lexicodes up to high dimensionalities. The graphs of the syndrome functions turn out to have curious fractal properties. As part of an on-going program investigating these functions, we consider them as polynomials in subfields of the quadratic closure of GF(2). Passing from such a polynomial function to its coefficient sequence provides a linear transform, analogous to the discrete Fourier transform. Despite the exponentially increasing sizes of the transform matrices, they may be inverted explicitly. The inverse transform matrices have a fractal structure, including the Sierpiński triangle in their first row. The paper "A Discrete Transform and Function Spaces on the Quadratic Closure of GF(2)" (Chap-

ter 3) studies the transform, and uses the transform to analyze certain spaces of natural number functions that include the syndromes of the codes. Transforms of functions in these spaces exhibit a martingale property.

Finally, Theorem 4.6 in Chapter 4 represents a key result on exponentiation in the quadratic closure of GF(2). It was originally proved by H. W. Lenstra, Jr. in 1980 [Le2]. We will give an alternative, more elementary approach to the proof of this result in Chapter 4.

Dissertation Organization

This dissertation includes two papers, entitled "Logarithms, Syndrome Functions, and the Information Rates of Greedy Loop Transversal Codes" and "A Discrete Transform and Function Spaces on the Quadratic Closure of GF(2)," Chapters 2 and 3 respectively. In Chapter 4, we study some additional properties of the quadratic closure of GF(2). Chapter 5 comprises the general conclusions. In the Bibliography, we list all the references we used in the previous chapters.

CHAPTER 2. LOGARITHMS, SYNDROME FUNCTIONS, AND THE INFORMATION RATES OF GREEDY LOOP TRANSVERSAL CODES

A paper accepted by the Journal of Combinatorial Mathematics
and Combinatorial Computing

Feng-Luan Hsu, Frank A. Hummer and Jonathan D. H. Smith[1]

Abstract

The paper studies linear block codes and syndrome functions built by the greedy loop transversal algorithm. The syndrome functions in the binary white-noise case are generalizations of the logarithm, with curious fractal properties. The codes in the binary white-noise case coincide with lexicodes: their dimensions are listed for channel lengths up to the sixties, and up to the three hundreds for double errors. In the ternary double-error case, record-breaking codes of lengths 43 to 68 are constructed.

[1]Graduate students and Professor, respectively, Department of Mathematics, Iowa State University.

Introduction

The general loop transversal approach to the construction of linear block codes was introduced in [Sm]. A companion paper [HmS] gives further details, concentrating on the greedy loop transversal algorithm in the binary case. In particular, it is shown there [HmS, Theorem 6.1] that the greedy loop transversal algorithm provides an alternative method for building binary lexicodes, especially suitable for good channels. The current paper has two aims. The first is to present data on the dimensions of the codes of various lengths constructed by the greedy loop transversal algorithm. (The phrase "loop transversal code" is abbreviated here to "LT code".) For binary channels, double, triple and quadruple white-noise error patterns are treated, corresponding to minimum distances 5, 6 (Table 2.2, 2.3, and 2.4) and 7–10 (Table 2.5) in metric language. The data may be read as giving the dimensions of lexicodes, for channel lengths beyond 300 in the double-error case. For ternary channels, greedy loop transversal codes and lexicodes differ, since the former are linear while the latter are not. Table 2.6 gives the dimensions of the ternary Hamming double-error correcting greedy loop transversal codes, for channel lengths up to 68. They include the perfect ternary Golay code, and new record-breaking codes for lengths above 42.

The second aim of the paper is to draw attention to the syndrome functions constructed by the greedy loop transversal algorithm for binary white-noise error patterns. For single errors, the syndrome (2.9) is essentially the logarithm function, so for other white-noise error patterns the syndromes may be considered as generalizations of the logarithm. Their graphs (Figures 2.1–2.6) display curious fractal properties that warrant further investigation. Another mysterious feature of the syndromes is the apparent convergence of the "efficiencies" defined below (2.11) and

recorded in Table 2.1.

The presentation of the graphical and tabular data in Sections 3 and 4 is prefaced by a description of the greedy loop transversal algorithm in Section 2, for arbitrary error patterns in channels over alphabets that are prime fields.

The greedy loop transversal algorithm

Fix a prime p. Each natural number n (including 0) has a unique expansion

$$n = \sum_{i=0}^{\infty} n(i)p^i \tag{2.1}$$

with $0 \leq n(i) < p$ for each i. Moreover, $n(i) = 0$ for $i > \lfloor \log_p n \rfloor$. For $d > \lfloor \log_p n \rfloor$, the natural number n may be identified with the vector $(n(d-1), \ldots, n(1), n(0))$ in the d-dimensional vector space $V_d = GF(p)^d$ over the Galois field $GF(p)$ of order p. Thus the set $\mathbf{N}$ of natural numbers is identified with the nested union $\bigcup_{d>0} V_d$ of vector spaces. The induced addition and subtraction operations on integers are written as $+_p$ and $-_p$ to avoid confusion with the usual addition and subtraction. For example, both $+_2$ and $-_2$ are the "nim sum" of [Co, p.51]. Besides the usual (well-)ordering $\leq$, the set of natural numbers carries a partial ordering $\subseteq_p$, known as the *Hamming order*, defined by

$$m \subseteq_p n \Leftrightarrow \exists F \subset \mathbf{N}. \quad m = n - \sum_{i \in F} n(i)p^i. \tag{2.2}$$

In other words, m is bounded above by n in the Hamming order if and only if the expansion (2.1) for m is obtained from the expansion for n by replacing certain digits $n(i)$ - namely those with i in F - by the digit 0. Note that 0 is the bottom element of $(\mathbf{N}, \subseteq_p)$, and that the Hamming distance between m and n is the rank of $m -_p n$ in the poset $(\mathbf{N}, \subseteq_p)$.

A subset X of a poset $(Y, \sqsubseteq)$ is said to be *self-subordinate* if $y \sqsubseteq x \in X$ implies $y \in X$. A self-subordinate subset E of $(\mathbf{N}, \subseteq_p)$ is called an *error pattern* if it contains the set $p^{\mathbf{N}} = \{p^i | i \in \mathbf{N}\}$. Error patterns model sets of errors to be corrected in the various channels V_d. For example, $\{\alpha p^i | \alpha \in GF(p); i \in \mathbf{N}\}$ comprises the errors of Hamming weight at most 1. White noise double errors are modeled by $\{\alpha p^i +_p \beta p^j | \alpha, \beta \in GF(p); i, j \in \mathbf{N}\}$. Burst double errors are modeled by $\{\alpha p^i +_p \beta p^j | \alpha, \beta \in GF(p); i, j \in \mathbf{N}, |i-j| \leq 1\}$. Error patterns form partial algebras under the operations of the vector space $(\mathbf{N}, +_p, GF(p))$. For example, the sum $p^i +_p p^j$ is defined in the burst double error pattern if and only if $|i - j| \leq 1$. Suppose that an error pattern E is given. Then an *E-syndrome*, or just *syndrome*, is a partial function $s : E \to \mathbf{N}$ which:

$$\begin{aligned} &(a) \quad \text{injects;} \\ &(b) \quad \text{is a partial vector space homomorphism;} \\ &(c) \quad \text{has domain self-subordinate in } (E, \leq), \text{ and} \\ &(d) \quad \text{satisfies: } \forall n \in \mathbf{N},\ \exists r \in \mathbf{N}.\ p^{\mathbf{N}} \cap s(V_d \cap E) \text{ spans } V_r. \end{aligned} \tag{2.3}$$

The syndrome is said to be *proper* if s is a properly partial function. In view of (c), this is equivalent to finiteness of the domain of s. For a proper syndrome, the *length* is defined to be

$$n = \max\{1 + \lfloor \log_p m \rfloor | m \in dom\ s\}. \tag{2.4}$$

The *redundancy* is defined to be

$$r = \max\{1 + \lfloor \log_p(ms) \rfloor | m \in dom\ s\}. \tag{2.5}$$

A proper syndrome s defines a *parity map*

$$\varepsilon_s : V_n \to V_r \tag{2.6}$$

by linearity and $p^i\varepsilon_s = p^i s$ for $i < n$. By (c), these values $p^i s$ are defined. Condition (b) guarantees that s agrees with ε_s on $V_n \cap E$. Condition (d) yields that ε_s surjects. Condition (a) guarantees that *dom* s embeds into V_r under ε_s. A code C_n in the channel V_n correcting the set $V_n \cap E$ of errors, and having dimension $n - r$, is then given as the kernel of ε_s.

The greedy loop transversal algorithm determines an E-syndrome s by the partial linearity (2.3) (b) and the greedy choice of $p^n s$ given that $s : (V_n \cap E) \to \mathbf{N}$ has already been defined. In other words, $p^n s$ is the minimal element of the set of integers m satisfying the requirement

$$\begin{aligned} &\forall e \neq f \in V_{n+1} \cap E, \qquad (2.7)\\ &e(n)m +_p (e -_p (e(n)p^n))s \;\neq\; f(n)m +_p (f -_p (f(n)p^n))s. \end{aligned}$$

Then for $e \in (V_{n+1} - (V_n \cup \{p^n\})) \cap E$,

$$es := e(n)(p^n s) \;+_p\; (e \;-_p\; (e(n)p^n)s. \qquad (2.8)$$

In (2.7) and (2.8), juxtaposition of an element of $GF(p)$ and an integer denotes the scalar multiple of that integer by the element of $GF(p)$. Note that the partial linearity requirement (2.3) (b) initializes the algorithm with $0s = 0$. If E is closed under scalar multiplication, then (2.7) may be simplified. The greedy algorithm picks $p^n s$ to be the least integer not in *anathema*, the set

$$\{es +_p fs \mid e, f \in V_n \cap E;\; p^n +_p e \in E\}$$

(cf. [Sm,(5.1)]).

Binary white-noise syndrome functions

If E is the binary white-noise single error pattern $\{0\} \cup 2^{\mathbf{N}}$, the greedy loop transversal algorithm builds the improper syndrome function s_1 with $0s_1 = 0$ and

$$s_1 : 2^N \to \mathbf{N};\ x \mapsto 1 + \log_2 x. \tag{2.9}$$

In this sense, the syndrome function for single errors is essentially the logarithm function. One may then regard the syndrome function s_t built by the greedy loop transversal algorithm for the binary white-noise t-error pattern E_t as a generalization of the logarithm function. To facilitate comparison with the logarithm function, the syndrome function

$$s_t : E_t \to \mathbf{N};\ x \mapsto y \tag{2.10}$$

is graphed with $\log_2 x$ on the ordinate and y on the abscissa in Figures 2.1, 2.3, and 2.5, for 2-error, 3-error, and 4-error cases. With a similar convention, the graph of s_1 would appear as a straight line of slope 1. Figures 2.2, 2.4, and 2.6 "plot the graphs of Figures 2.1, 2.3, and 2.5 on logarithmic paper", i.e., they graph $s_t : x \mapsto y$ by plotting $\log_2 \log_2 x$ against $\log_2 y$. The fractal form of Figures 2.1–2.6 is very striking, and clearly warrants further investigation. As an initial step in such an investigation, define a *nodal point* of the syndrome function s_t to be a point on its graph of the form $(2^{n-1}, 2^k)$ for integral n, k. (The analysis given in [HmS] shows that the graph includes such points.) The proper syndrome given by the restriction of s_t to the channel V_n then yields a t-error correcting code C_n with redundancy $k+1$. By the sphere-packing bound,

$$2^{k+1} \geq \binom{n}{t} + \binom{n}{t-1} + \ldots + \binom{n}{1} + \binom{n}{0}. \tag{2.11}$$

The *efficiency* of the code C_n of redundancy $k+1$ is the ratio of $\log_2[\binom{n}{t} + \binom{n}{t-1} + \ldots + \binom{n}{1} + \binom{n}{0}]$ to $(k+1)$, usually expressed as a percentage. Table 2.1 lists these efficiencies for $0 < k < 19$ and $1 < t < 5$. Their apparent convergence to about 80% is rather curious.

Table 2.1: Efficiency of binary 2-, 3-, and 4-error greedy LT codes

$k+1$	2-Error	3-Error	4-Error
19	79.61	79.67	79.76
18	79.73	82.44	79.71
17	79.99	78.74	78.90
16	80.31	77.64	80.51
15	80.63	78.98	79.89
14	80.57	82.34	80.70
13	80.64	87.37	84.02
12	80.08	93.19	84.12
11	80.58	85.86	87.57
10	79.89	82.24	91.34
9	82.51	82.88	95.47
8	78.80	87.78	91.86
7	78.91	93.42	94.71
6	80.97	89.87	97.21
5	89.19	94.01	99.08
4	86.49	97.67	100.00
3	93.58	100.00	100.00
2	100.00	100.00	100.00

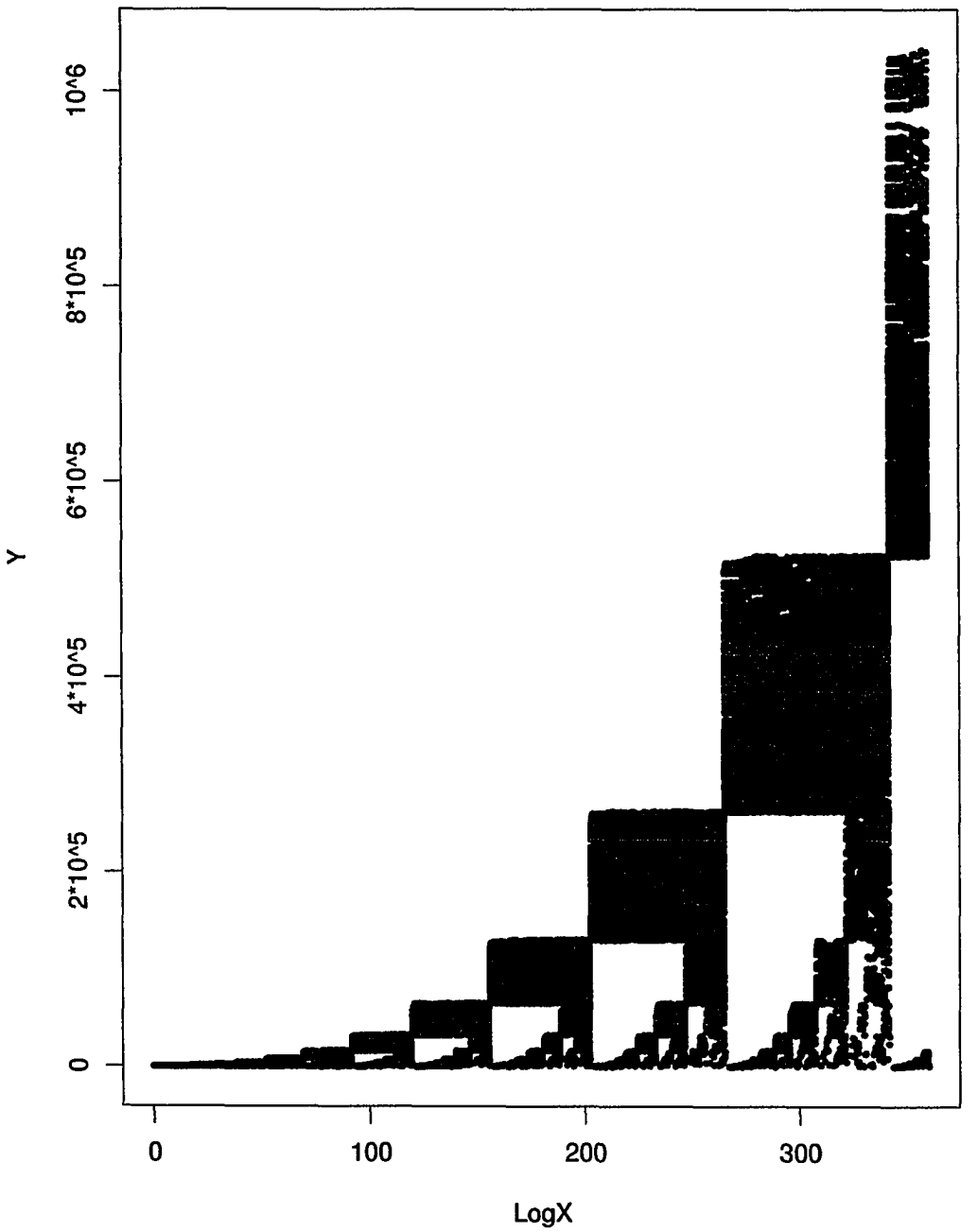

Figure 2.1: Syndrome function for binary 2-error

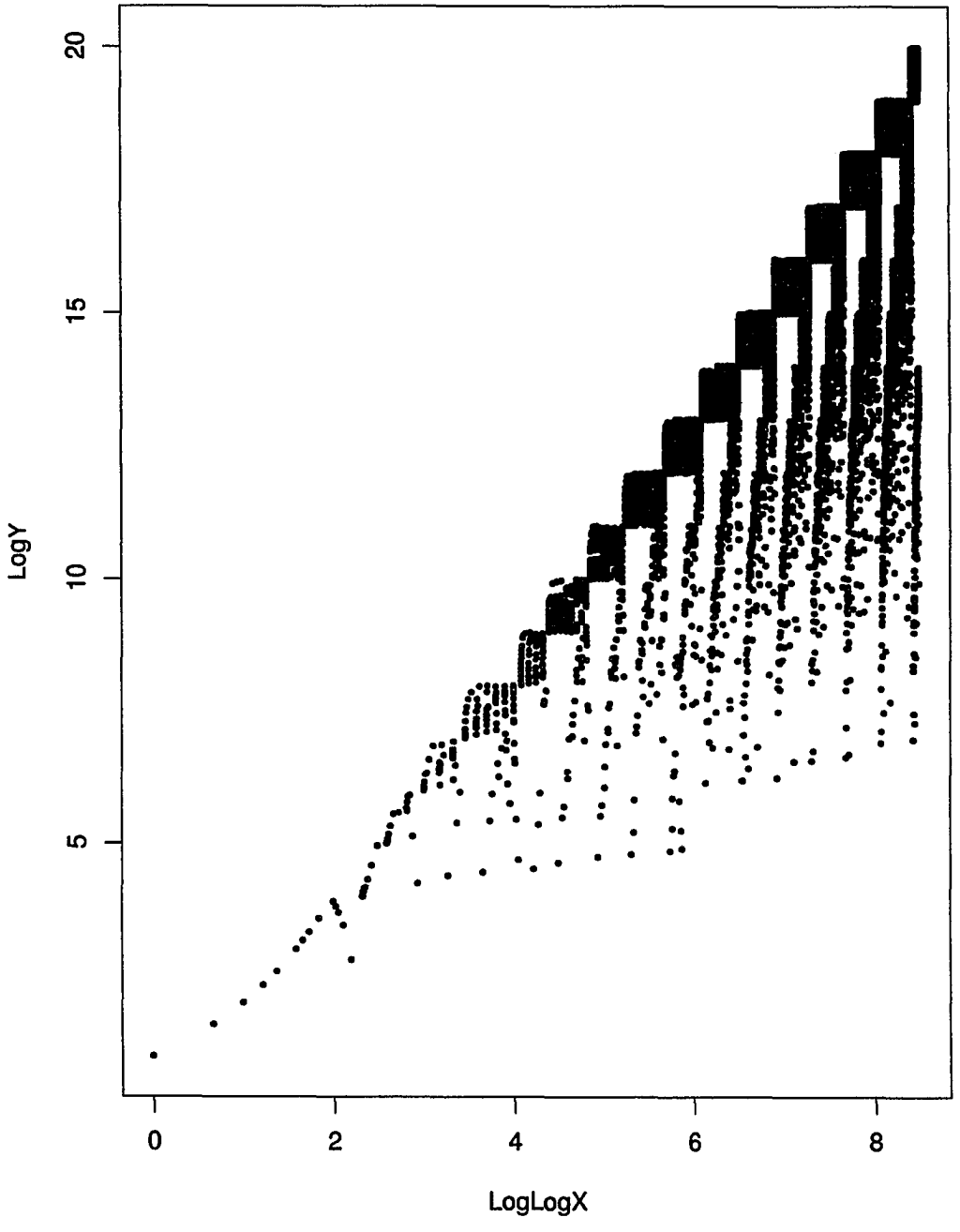

Figure 2.2: Syndrome function for binary 2-error

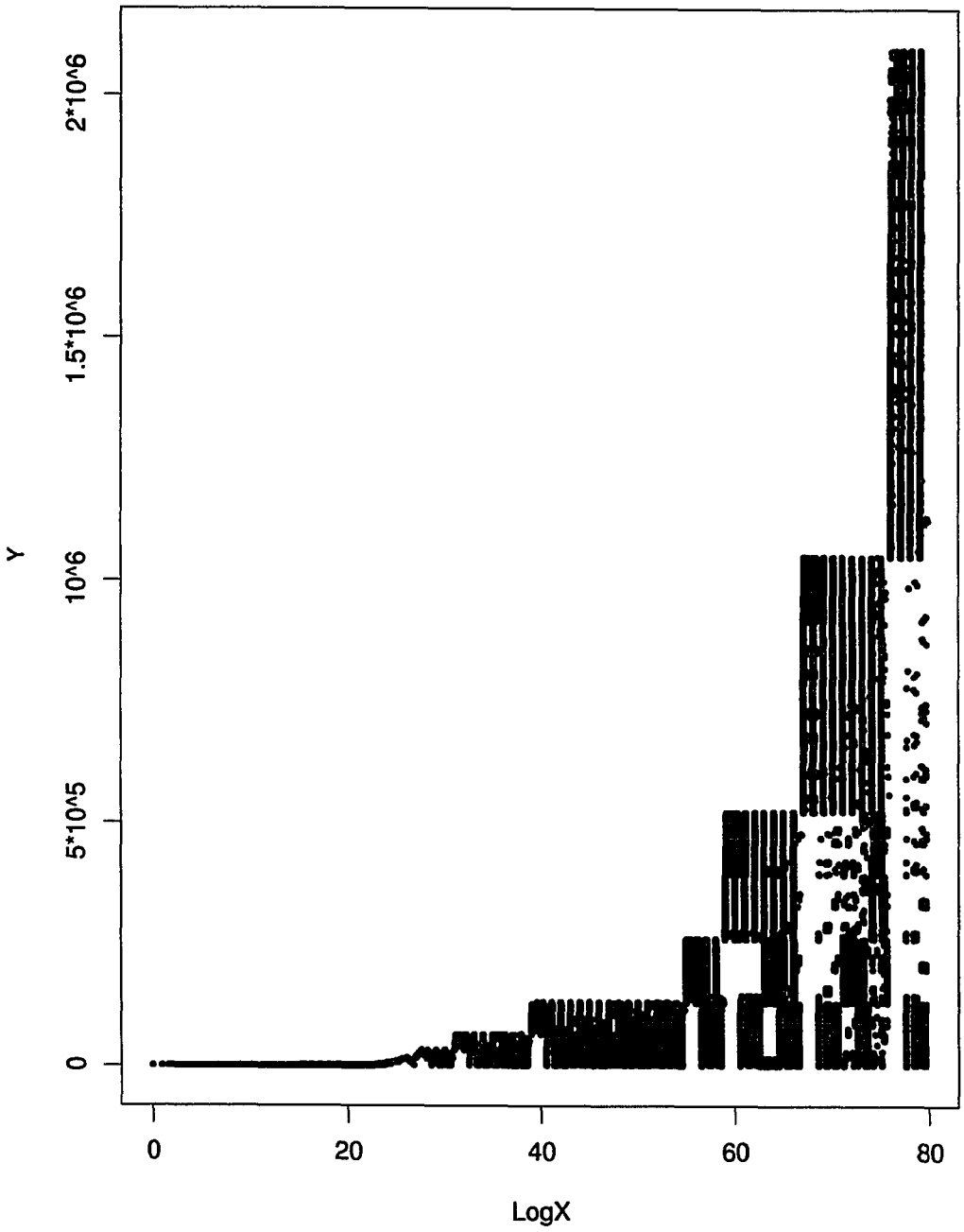

Figure 2.3: Syndrome function for binary 3-error

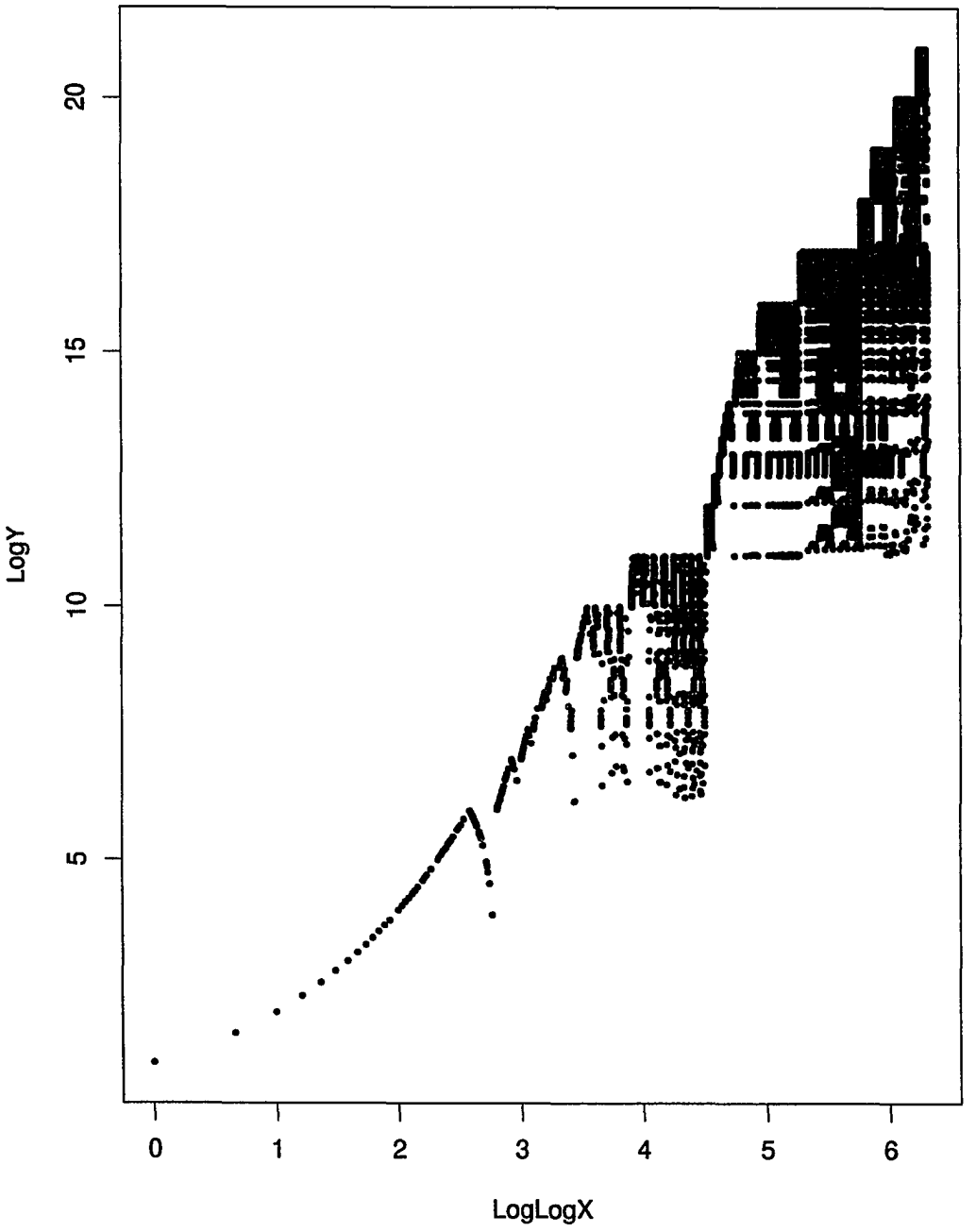

Figure 2.4: Syndrome function for binary 3-error

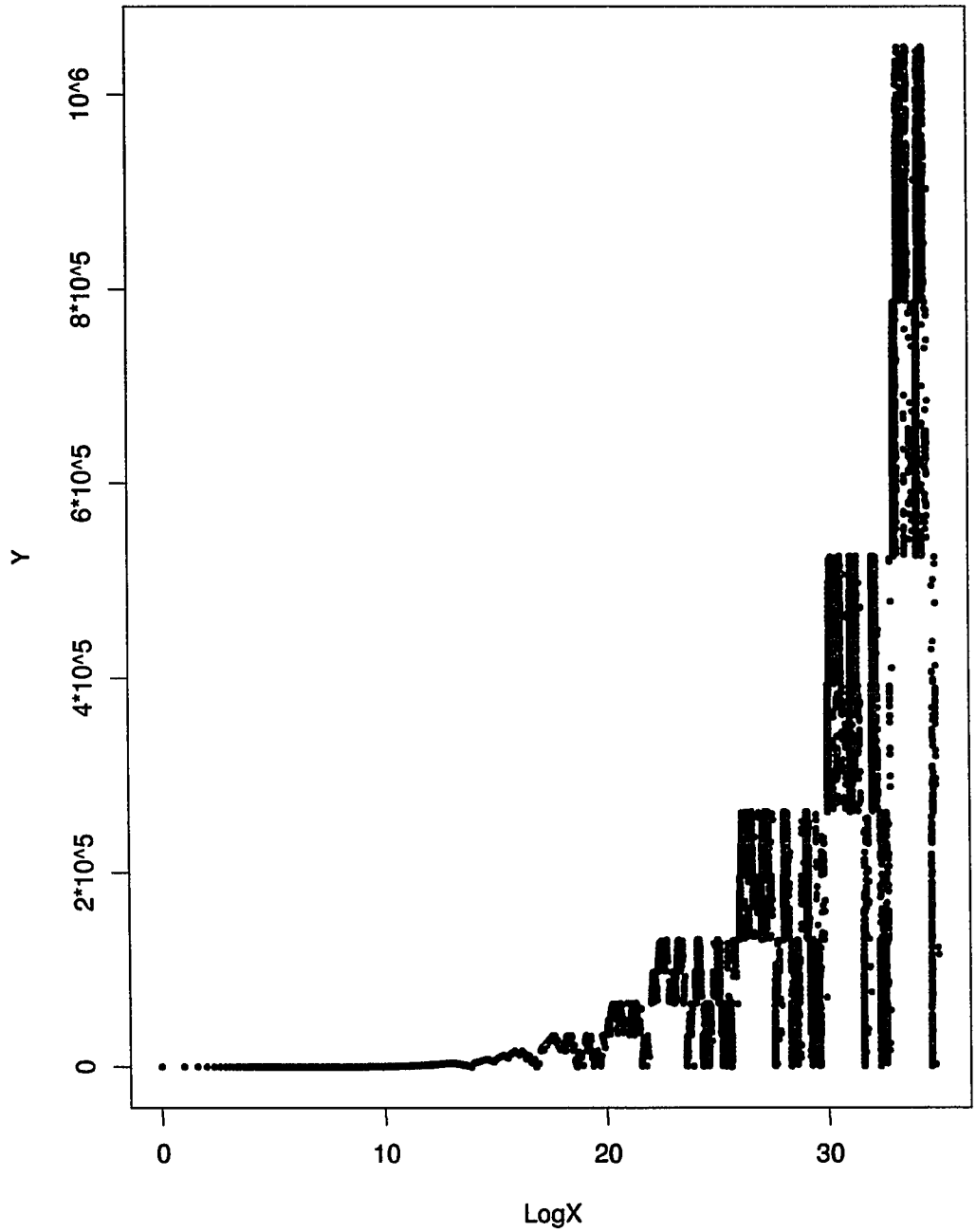

Figure 2.5: Syndrome function for binary 4-error

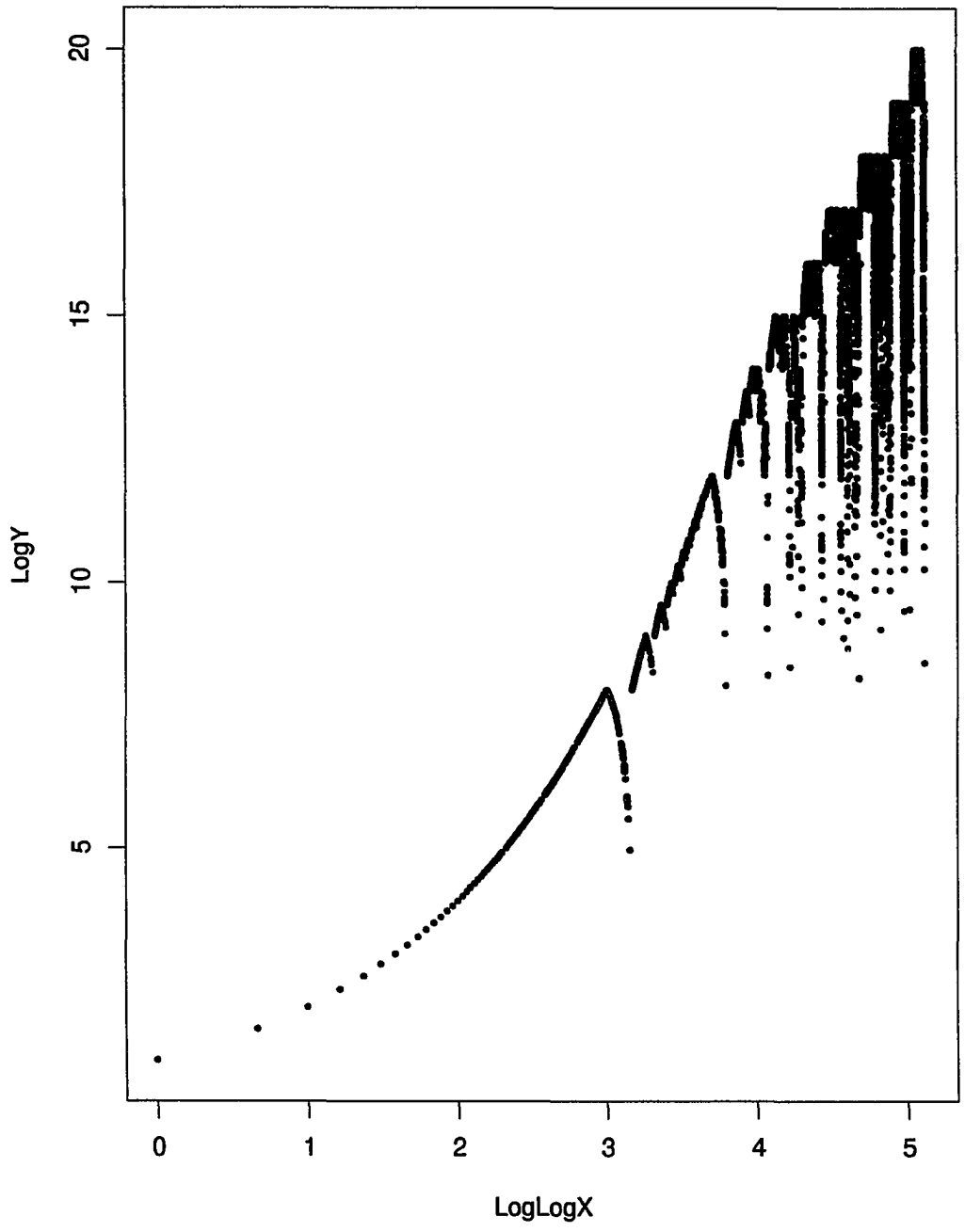

Figure 2.6: Syndrome function for binary 4-error

Dimensions of greedy LT codes

The final three tables record the dimensions of the codes C_n of length n constructed by the greedy loop transversal algorithm. For each n, the second column of Table 2.2, 2.3, and 2.4 records the dimension of the greedy LT code correcting binary white-noise double errors, i.e. of minimum Hamming distance $d = 5$. The third column records the dimension of the corresponding codes of minimum Hamming distance $d = 6$ obtained by adjoining a parity check (thus increasing the length by 1). For lengths less than 2^7, the entries in parentheses are the dimensions of the best known linear code of length n and minimum distance d, as recorded in [Ve]. Table 2.5 records analogous data for binary white-noise triple and quadruple errors, i.e. minimum distances $d = 7, 8, 9, 10$. Since binary greedy LT codes are the same as lexicodes [Theorem 6.1], Tables 2.2, 2.3, 2.4, and 2.5 may also be read as giving the dimensions of lexicodes. Table 2.6 lists the dimensions of the ternary greedy LT codes correcting white-noise Hamming double errors, i.e. with minimum Hamming distance $d = 5$. It is interesting to note that the code of length 11 has dimension 6, so that it coincides with the perfect ternary Golay code. The numbers in parentheses list the dimensions of the best known ternary linear codes of minimum distance 5, as recorded in [KP]. The greedy LT codes of lengths 43 to 50 are better than the best known to Kschischang and Pasupathy. The data in [KP] stopped at length 50, but the greedy LT codes of lengths 51 onwards are also likely to be world records.

Table 2.2: Dimensions of binary greedy LT codes

n	$d=5$	$d=6$	n	$d=5$	$d=6$	n	$d=5$	$d=6$
12	4(4)	4(4)	43	31(31)	30(30)	74	60(61)	59(60)
13	5(5)	4(4)	44	32(32)	31(31)	75	61(61)	60(61)
14	6(6)	5(5)	45	33(33)	32(32)	76	62(62)	61(61)
15	7(7)	6(6)	46	34(34)	33(33)	77	63(63)	62(62)
16	8(8)	7(7)	47	35(35)	34(34)	78	64(64)	63(63)
17	9(9)	8(8)	48	36(36)	35(35)	79	65(65)	64(64)
18	9(9)	9(9)	49	37(37)	36(36)	80	66(66)	65(65)
19	10(10)	9(9)	50	38(38)	37(37)	81	67(67)	66(66)
20	11(11)	10(10)	51	39(39)	38(38)	82	68(68)	67(67)
21	12(12)	11(11)	52	40(40)	39(39)	83	69(69)	68(68)
22	12(13)	12(12)	53	41(41)	40(40)	84	70(70)	69(69)
23	13(14)	12(13)	54	41(42)	41(41)	85	71(71)	70(70)
24	14(14)	13(14)	55	42(43)	41(42)	86	72(72)	71(71)
25	15(15)	14(14)	56	43(44)	42(43)	87	73(73)	72(72)
26	16(16)	15(15)	57	44(45)	43(44)	88	74(74)	73(73)
27	17(17)	16(16)	58	45(46)	44(45)	89	75(75)	74(74)
28	18(18)	17(17)	59	46(47)	45(46)	90	76(76)	75(75)
29	19(19)	18(18)	60	47(48)	46(47)	91	77(77)	76(76)
30	19(20)	19(19)	61	48(49)	47(48)	92	78(78)	77(77)
31	20(21)	19(20)	62	49(50)	48(49)	93	78(79)	78(78)
32	21(22)	20(21)	63	50(51)	49(50)	94	79(80)	78(79)
33	22(22)	21(22)	64	51(52)	50(51)	95	80(81)	79(80)
34	23(23)	22(22)	65	52(53)	51(52)	96	81(82)	80(81)
35	24(24)	23(23)	66	53(53)	52(53)	97	82(83)	81(82)
36	25(25)	24(24)	67	54(54)	53(53)	98	83(84)	82(83)
37	26(26)	25(25)	68	55(55)	54(54)	99	84(85)	83(84)
38	27(27)	26(26)	69	56(56)	55(55)	100	85(86)	84(85)
39	27(28)	27(27)	70	56(57)	56(56)	101	86(87)	85(86)
40	28(29)	27(28)	71	57(58)	56(57)	102	87(88)	86(87)
41	29(30)	28(29)	72	58(59)	57(58)	103	88(89)	87(88)
42	30(30)	29(30)	73	59(60)	58(59)	104	89(90)	88(89)

Note: numbers inside ( ) are data from Tom Verhoeff in IEEE 1987

Table 2.3: Dimensions of binary greedy LT codes

n	$d=5$	$d=6$	n	$d=5$	$d=6$	n	$d=5$	$d=6$
105	90(91)	89(90)	142	126	125	179	162	161
106	91(92)	90(91)	143	127	126	180	163	162
107	92(93)	91(92)	144	128	127	181	164	163
108	93(94)	92(93)	145	129	128	182	165	164
109	94(95)	93(94)	146	130	129	183	166	165
110	95(96)	94(95)	147	131	130	184	167	166
111	96(97)	95(96)	148	132	131	185	168	167
112	97(98)	96(97)	149	133	132	186	169	168
113	98(99)	97(98)	150	134	133	187	170	169
114	99(100)	98(99)	151	135	134	188	171	170
115	100(101)	99(100)	152	136	135	189	172	171
116	101(102)	100(101)	153	137	136	190	173	172
117	102(103)	101(102)	154	138	137	191	174	173
118	103(104)	102(103)	155	139	138	192	175	174
119	104(105)	103(104)	156	140	139	193	176	175
120	105(106)	104(105)	157	140	140	194	177	176
121	105(107)	105(106)	158	141	140	195	178	177
122	106(108)	105(107)	159	142	141	196	179	178
123	107(109)	106(108)	160	143	142	197	180	179
124	108(110)	107(109)	161	144	143	198	181	180
125	109(111)	108(110)	162	145	144	199	182	181
126	110(112)	109(111)	163	146	145	200	183	182
127	111(113)	110(112)	164	147	146	201	184	183
128	112	111	165	148	147	202	185	184
129	113	112	166	149	148	203	186	185
130	114	113	167	150	149	204	186	186
131	115	114	168	151	150	205	187	186
132	116	115	169	152	151	206	188	187
133	117	116	170	153	152	207	189	188
134	118	117	171	154	153	208	190	189
135	119	118	172	155	154	209	191	190
136	120	119	173	156	155	210	192	191
137	121	120	174	157	156	211	193	192
138	122	121	175	158	157	212	194	193
139	123	122	176	159	158	213	195	194
140	124	123	177	160	159	214	196	195
141	125	124	178	161	160	215	197	196

Table 2.4: Dimensions of binary greedy LT codes

n	$d=5$	$d=6$	n	$d=5$	$d=6$	n	$d=5$	$d=6$	n	$d=5$	$d=6$
216	198	197	253	235	234	290	271	270	327	308	307
217	199	198	254	236	235	291	272	271	328	309	308
218	200	199	255	237	236	292	273	272	329	310	309
219	201	200	256	238	237	293	274	273	330	311	310
220	202	201	257	239	238	294	275	274	331	312	311
221	203	202	258	240	239	295	276	275	332	313	312
222	204	203	259	241	240	296	277	276	333	314	313
223	205	204	260	242	241	297	278	277	334	315	314
224	206	205	261	243	242	298	279	278	335	316	315
225	207	206	262	244	243	299	280	279	336	317	316
226	208	207	263	245	244	300	281	280	337	318	317
227	209	208	264	246	245	301	282	281	338	319	318
228	210	209	265	247	246	302	283	282	339	320	319
229	211	210	266	248	247	303	284	283	340	321	320
230	212	211	267	248	248	304	285	284	341	322	321
231	213	212	268	249	248	305	286	285	342	323	322
232	214	213	269	250	249	306	287	286	343	323	323
233	215	214	270	251	250	307	288	287	344	324	323
234	216	215	271	252	251	308	289	288	345	325	324
235	217	216	272	253	252	309	290	289	346	326	325
236	218	217	273	254	253	310	291	290	347	327	326
237	219	218	274	255	254	311	292	291	348	328	327
238	220	219	275	256	255	312	293	292	349	329	328
239	221	220	276	257	256	313	294	293	350	330	329
240	222	221	277	258	257	314	295	294	351	331	330
241	223	222	278	259	258	315	296	295	352	332	331
242	224	223	279	260	259	316	297	296	353	333	332
243	225	224	280	261	260	317	298	297	354	334	333
244	226	225	281	262	261	318	299	298	355	335	334
245	227	226	282	263	262	319	300	299	356	336	335
246	228	227	283	264	263	320	301	300	357	337	336
247	229	228	284	265	264	321	302	301	358	338	337
248	230	229	285	266	265	322	303	302	359	339	338
249	231	230	286	267	266	323	304	303	360	340	339
250	232	231	287	268	267	324	305	304			
251	233	232	288	269	268	325	306	305			
252	234	233	289	270	269	326	307	306			

Table 2.5: Dimensions of binary greedy LT codes

n	$d=7$	$d=8$	$d=9$	$d=10$	n	$d=7$	$d=8$
12	2(2)	2(2)	1(1)	1(1)	41	24(25)	23(24)
13	3(3)	2(2)	1(1)	1(1)	42	25(26)	24(25)
14	4(4)	3(3)	2(2)	1(1)	43	26(27)	25(26)
15	5(5)	4(4)	2(2)	2(2)	44	27(28)	26(27)
16	5(5)	5(5)	2(2)	2(2)	45	28(29)	27(28)
17	6(6)	5(5)	3(3)	2(2)	46	29(30)	28(29)
18	7(7)	6(6)	3(3)	3(3)	47	30(31)	29(30)
19	8(8)	7(7)	4(4)	3(3)	48	31(31)	30(31)
20	9(9)	8(8)	5(5)	4(4)	49	32(32)	31(31)
21	10(10)	9(9)	5(5)	5(5)	50	33(33)	32(32)
22	11(11)	10(10)	6(6)	5(5)	51	34(34)	33(33)
23	12(12)	11(11)	6(7)	6(6)	52	35(35)	34(34)
24	12(12)	12(12)	7(7)	6(7)	53	36(36)	35(35)
25	12(12)	12(12)	8(8)	7(7)	54	37(37)	36(36)
26	12(13)	12(12)	9(9)	8(8)	55	38(38)	37(37)
27	13(14)	12(13)	9(10)	9(9)	56	38(39)	38(38)
28	13(14)	13(14)	10(10)	9(10)	57	39(40)	38(39)
29	14(15)	13(14)	11(11)	10(10)	58	40(41)	39(40)
30	15(16)	14(15)	12(12)	11(11)	59	41(42)	40(41)
31	16(17)	15(16)	12(12)	12(12)	60	41(43)	41(42)
32	16(17)	16(17)	13(13)	12(12)	61	42(44)	41(43)
33	17(18)	16(17)	14(14)	13(13)	62	43(45)	42(44)
34	18(19)	17(18)		14(14)	63	44(46)	43(45)
35	19(20)	18(19)			64		44(46)
36	20(20)	19(20)					
37	21(21)	20(20)					
38	22(22)	21(21)					
39	23(23)	22(22)					
40	23(24)	23(23)					

Table 2.6: Dimensions of ternary greedy LT 2-error codes

n	$d=5$	n	$d=5$	n	$d=5$
5	1(1)	27	18(19)	49	39(38)
6	1(1)	28	19(20)	50	40(39)
7	2(2)	29	20(21)	51	41
8	3(3)	30	21(22)	52	42
9	4(4)	31	22(23)	53	43
10	5(5)	32	23(24)	54	44
11	6(6)	33	24(25)	55	45
12	6(6)	34	25(26)	56	46
13	6(6)	35	26(27)	57	47
14	6(7)	36	27(28)	58	48
15	8(8)	37	28(29)	59	49
16	8(9)	38	29(30)	60	50
17	9(10)	39	30(31)	61	51
18	10(11)	40	31(32)	62	52
19	11(12)	41	32(33)	63	53
20	12(13)	42	33(33)	64	54
21	13(14)	43	34(33)	65	55
22	14(15)	44	35(33)	66	56
23	15(16)	45	36(34)	67	57
24	16(17)	46	37(35)	68	58
25	16(18)	47	37(36)	69	
26	17(19)	48	38(37)	70	

Note: numbers inside ( ) are data from Kschischang and Pasupathy in IEEE 1992

References

[Co] J.H.Conway, *On Numbers and Games*, Camb. Univ. Press, Cambridge, 1975.

[HS] F.A. Hummer and J.D.H. Smith, *Greedy loop transversal codes,metrics, and lexicodes*, Journal of Combinatorial Mathematics and Combinatorial Computing.

[KP] F.R. Kschischang and S. Pasupathy,*Some ternary and quaternary codes and associated sphere packings*,I.E.E.E. Trans. Info. Th. **IT-38**,(1992), 227–246.

[Sm] J.D.H. Smith, *Loop transversals to linear codes*, J. Comb., Info. and Syst. Sci. **17** (1992), 1-8.

[Ve] T. Verhoeff *An updated table of minimum-distance bounds for binary linear codes*, I.E.E.E. Trans. Info. Th. **IT-33** (1987), 665–680

CHAPTER 3. A DISCRETE TRANSFORM AND FUNCTION SPACES ON THE QUADRATIC CLOSURE OF GF(2)

A paper submitted for publication
to Discrete Mathematics Feng-Luan Hsu and Jonathan D. H. Smith [1]

Abstract

The construction of syndrome functions for binary error-correcting codes using greedy algorithms yields sequences of linear endomorphisms of Galois fields that are successive quadratic extensions of the two-element field. As part of the analysis of such endomorphisms, this paper introduces and studies a linear transform of them, analogous to the discrete Fourier transform. Although the matrices of the transforms are non-sparse and increase in size exponentially, they can all be inverted explicitly. The inverse transform matrices have a fractal structure, including the Sierpiński triangle in their first row. The paper uses the transform to analyze certain spaces of natural number functions that include the syndromes of the codes. Transforms of functions in these spaces exhibit a martingale property.

[1]Graduate student and Professor, respectively, Department of Mathematics, Iowa State University.

Introduction

A general "loop transversal" approach to the construction of linear block codes was introduced in [Sm]. A subsequent paper [HS] gives further details, concentrating on the greedy loop transversal algorithm in the binary case. The greedy algorithm was used in [HHS] to construct syndrome functions of binary lexicodes up to high dimensionalities. The graphs of the syndrome functions turn out to have curious fractal properties. As part of an on-going program investigating these functions, we consider them as polynomials in subfields of the quadratic closure of GF(2). Passing from such a polynomial function to its coefficient sequence provides a linear transform, analogous to the discrete Fourier transform. Despite the exponentially increasing sizes of the transform matrices, they may be inverted explicitly. The current paper is devoted to a detailed analysis of the transform.

It proves convenient to identify the quadratic closure of GF(2) with the (ordered) set $\mathbf{N}$ of natural numbers. Thus $\mathbf{N}$ becomes a subfield of the Field $\mathbf{On_2}$ introduced by Conway [Co, Chapter 6] [Le], and the finite field $\mathrm{GF}(2^{2^n})$ becomes $\{n \in \mathbf{N} | n < 2^{2^n}\}$. Note that $\{2^0, 2^1, \ldots, 2^{2^n-1}\}$ is a basis of the GF(2)-space $\mathrm{GF}(2^{2^n})$. Moreover, the GF(2)-endomorphisms $x \mapsto x^{2^0}$, $x \mapsto x^{2^1}, \ldots, x \mapsto x^{2^{2^n-1}}$ are linearly independent in the $\mathrm{GF}(2^{2^n})$-space of functions $\mathrm{GF}(2^{2^n}) \to \mathrm{GF}(2^{2^n})$. Thus a GF(2)-linear function $h : \mathrm{GF}(2^{2^n}) \to \mathrm{GF}(2^{2^n})$ can be written in the form

$$\begin{aligned} h(x) &= a_{n,0}x^{2^0} + a_{n,1}x^{2^1} + a_{n,2}x^{2^2} + \ldots + a_{n,2^n-1}x^{2^{2^n-1}} \\ &= (x^{2^0}, x^{2^1}, x^{2^2}, \ldots, x^{2^{2^n-1}})(a_{n,0}, a_{n,1}, a_{n,2}, \ldots, a_{n,2^n-1})^T. \end{aligned}$$

To describe such a linear function $h(x)$, one only needs to look at the function values

$h(2^i)$, for $0 \leq i \leq 2^n - 1$. So we have

$$\begin{bmatrix} (2^0)^{2^0} & (2^0)^{2^1} & \ldots & (2^0)^{2^{2^n-1}} \\ (2^1)^{2^0} & (2^1)^{2^1} & \ldots & (2^1)^{2^{2^n-1}} \\ \vdots & \vdots & \vdots & \ldots \quad \vdots \\ (2^{2^n-1})^{2^0} & (2^{2^n-1})^{2^1} & \ldots & (2^{2^n-1})^{2^{2^n-1}} \end{bmatrix} \begin{bmatrix} a_{n,0} \\ a_{n,1} \\ \vdots \\ a_{n,2^n-1} \end{bmatrix} = \begin{bmatrix} h(2^0) \\ h(2^1) \\ \vdots \\ h(2^{2^n-1}) \end{bmatrix}.$$

Now, multiplying both sides of the equation by the inverse f_n^{-1} of the $2^n \times 2^n$ matrix f_n on the left, one obtains the function values of a new linear function $\breve{h}$:

$$\begin{aligned} & [\breve{h}(2^0),\ \breve{h}(2^1),\ \breve{h}(2^2),\ \ldots,\ \breve{h}(2^{2^n-1})]^T \\ = \ & [a_{n,0},\ a_{n,1},\ a_{n,2},\ \ldots\ a_{n,2^n-1}]^T \\ = \ & \begin{bmatrix} (2^0)^{2^0} & (2^0)^{2^1} & (2^0)^{2^2} & \ldots & (2^0)^{2^{2^n-1}} \\ (2^1)^{2^0} & (2^1)^{2^1} & (2^1)^{2^2} & \ldots & (2^1)^{2^{2^n-1}} \\ (2^2)^{2^0} & (2^2)^{2^1} & (2^2)^{2^2} & \ldots & (2^2)^{2^{2^n-1}} \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ (2^{2^n-1})^{2^0} & (2^{2^n-1})^{2^1} & (2^{2^n-1})^{2^2} & \ldots & (2^{2^n-1})^{2^{2^n-1}} \end{bmatrix}^{-1} \begin{bmatrix} h(2^0) \\ h(2^1) \\ h(2^2) \\ \vdots \\ h(2^{2^n-1}) \end{bmatrix} \\ = \ & f_n^{-1}[h(2^0),\ h(2^1),\ h(2^2),\ \ldots,\ h(2^{2^n-1})]^T. \end{aligned}$$

Passing from the linear function h to the linear function $\breve{h}$ provides the 2^n-dimensional linear transform, an analogue of the discrete Fourier transform. For example, the field GF(2^{16}) becomes $\{n \in \mathbf{N} | n < 2^{16}\}$. Using hexadecimal notation for these numbers, Table 3.1 displays the 16×16 transform matrix f_4. Note that the number in the $(i+1,\ j)$-entry is the square of the number in the $(i,\ j)$-entry, for $1 \leq i \leq 15, 1 \leq j \leq 16$. Here the square is taken in GF(2^{16}). So it will be enough to construct the whole matrix if we know the entries $(1,\ j)$, for $1 \leq j \leq 16$, i.e. the first row of the matrix. In Table 3.2 , we transform the numbers in the first row of the matrix into

binary format, and transpose the row to a column. Observe that the numbers form a Sierpiński triangle, i.e. Pascal's Triangle modulo 2. For any n, we have similar results. If we denote the rows of Pascal's Triangle modulo 2, namely 1, 3, 5, F, 11, 33, 55, ... (in hexadecimal format), by $P_0 = 1,\ P_1 = 3,\ P_3 = 5, ...$, then we have f_n^{-1} of the form

$$\begin{bmatrix} P_{2^n-1} & P_{2^n-2} & P_{2^n-3} & \dots & P_0 \\ P_{2^n-1}\varphi & P_{2^n-2}\varphi & P_{2^n-3}\varphi & \dots & P_0\varphi \\ P_{2^n-1}\varphi^2 & P_{2^n-2}\varphi^2 & P_{2^n-3}\varphi^2 & \dots & P_0\varphi^2 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ P_{2^n-1}\varphi^{2^n-1} & P_{2^n-2}\varphi^{2^n-1} & P_{2^n-3}\varphi^{2^n-1} & \dots & P_0\varphi^{2^n-1} \end{bmatrix},$$

where $x\varphi^k = x^{2^k}$ for each $n > 0$.

In Section 2, we describe the order and field structure on $\mathbf{N}$. In Section 3, we discuss relevant properties of Pascal's Triangle modulo 2. The structure of the inverse transform matrix is determined in Section 4 and Section 5. In Section 6, we examine subspaces of the GF(2)-space $\prod_{n=0}^{\infty}$End GF(2^{2^n}) defined by certain properties of their elements, namely coherence, smallness, the nesting property and the martingale property. These properties are displayed by the syndrome functions of binary lexicodes. We show that the martingale property is equivalent to coherence, and that the smallness, coherence and nesting properties are independent of each other. The final section completes the investigation of the relationship between these properties.

Order and field structures on N

For $k \in \mathbf{N}$, write $k = \sum_{i=0}^{\infty} k_i 2^i$ with $k_i \in \{0, 1\}$. Then we have a bijection $\mathbf{N} \to \amalg_{i=0}^{\infty}$ GF(2); $k \mapsto \sum_{i=0}^{\infty} k_i$. Using this bijection, we can make $\mathbf{N}$ a GF(2)-space.

The induced addition on $\mathbf{N}$ is called *nim addition* (to contrast with the usual addition on $\mathbf{N}$), because of its role in the analysis of the game of Nim [Co, Chapter 11]. In this paper, we will use $\sum$ and $+$ for nim addition and use $-$ for ordinary subtraction. Note that the ordinary addition can always be written in terms of subtraction. For example, the ordinary sum of a and b will be represented by $a-(-b)$.

Let $(\mathbf{N},\leq)$ be the usual linear order on the natural numbers. For $a,b\in\mathbf{N}$, we then use the following "interval" notations : "open" $(a,b):=\{n\in\mathbf{N}|a<n<b\}$, "closed above" $(a,b]:=\{n\in\mathbf{N}|a<n\leq b\}$, " closed below" $[a,b):=\{n\in\mathbf{N}|a\leq n<b\}$, "closed" $[a,b]:=\{n\in\mathbf{N}|a\leq n\leq b\}$. Occasionally, it is convenient to identify b with $[0,b)$, e.g. writing GF(2)$=0,1$ simply as 2.

The essential property of nim addition which we need is that for any three natural numbers α, β, γ, with $\gamma<\alpha+\beta$, there exists $\alpha'<\alpha$ with $\alpha'+\beta=\gamma$ or $\beta'<\beta$ with $\alpha+\beta'=\gamma$. Since for $\alpha'\neq\alpha$, $\beta'\neq\beta$, we have $\alpha'+\beta\neq\alpha+\beta\neq\alpha+\beta'$, it follows that

$\alpha+\beta$ is the smallest natural number different from all natural numbers

$$\alpha'+\beta \text{ with } \alpha'<\alpha \text{ and from all } \alpha+\beta' \text{ with } \beta'<\beta. \qquad (3.1)$$

It was noticed by Conway that this property may in fact be taken as a recursive definition of nim addition. As Conway remarks, nim addition is in a sense the "simplest" addition making the natural numbers into a group. The same thing happens for the binary operation $*$ known as *nim multiplication.* The basic inequality to be used here expresses the absence of zero-divisors, i.e. $(\alpha+\alpha')*(\beta+\beta')\neq 0$, for $\alpha\neq\alpha',\beta\neq\beta'$. So $\alpha*\beta\neq\alpha'*\beta+\alpha*\beta'+\alpha'*\beta'$. This leads to the following definition of nim

multiplication, due to Conway :

$\alpha * \beta$ is the smallest natural number different from all natural numbers

$$(\alpha' * \beta) + (\alpha * \beta') + (\alpha' * \beta') \text{ with } \alpha' < \alpha, \text{ and } \beta' < \beta. \quad (3.2)$$

Efficient algorithms to aid in the computation of the nim sum $x + y$ and the nim product $x * y$ of two natural numbers x, y are as follows:

$$\textbf{if} \quad x = y \quad \textbf{then} \quad x + y = 0 \quad \textbf{else} \quad (3.3)$$

$$\textbf{if} \quad \exists n \in \mathbf{N}. \quad y < x = 2^n \quad \textbf{then}$$

$$x + y \text{ is the ordinary sum of } x \text{ and } y.$$

$$\textbf{if} \quad \exists n \in \mathbf{N}. \quad x = 2^{2^n} \quad \textbf{then} \quad (3.4)$$

$$\textbf{if } x = y \quad \textbf{then} \quad x * y \text{ is the ordinary product of } \frac{3}{2} \text{ and } x$$

$$\textbf{else if} \quad y < x \quad \textbf{then} \quad x * y \text{ is the ordinary product of } x \text{ and } y.$$

The algorithms are complemented by the distributive laws. As an example of the use of the algorithms, one obtains $2^{2^n+k} = 2^{2^n} * 2^k$ for $k < 2^n$.

Theorem 3.1 [Co, Theorem 49] *The set* $\mathbf{N}$ *of natural numbers, with nim addition and nim multiplication, is a quadratically closed field of characteristic 2, the quadratic closure of* GF(2).

In this paper, we will write $\prod_{i=0}^{r} a_i$ for the iterated nim product $a_0 * a_1 * \ldots * a_r$. We also set $\alpha_n = 2^{2^n}$ and $\beta_n = \prod_{i=0}^{n-1} \alpha_i$. Note $\mathrm{GF}(\alpha_0) < \mathrm{GF}(\alpha_1) < \mathrm{GF}(\alpha_2) < \ldots$, and $\mathbf{N} = \cup_{i \geq 0} \mathrm{GF}(\alpha_i)$. Also, α_i satisfies the equation

$$x_i^2 + x_i + \prod_{j<i} \alpha_j = x_i^2 + x_i + \beta_{i-1} = 0, \quad (3.5)$$

so that $\mathrm{GF}(\alpha_i)$ is the quadratic extension $\mathrm{GF}(\alpha_{i-1})[\alpha_i]$.

Proposition 3.2 *The map* $\varphi : (\mathbf{N}, +, *) \to (\mathbf{N}, +, *)$; $a \mapsto a^2$ *is an automorphism of the field* **N**.

PROOF. Let a and b be natural numbers. Then :

1. $(a+b)\varphi = (a+b)^2 = a^2 + a*b + a*b + b^2 = a^2 + b^2 = a\varphi + b\varphi$;
2. $(a*b)\varphi = (a*b)^2 = (a*b)*(a*b) = (a*a)*(b*b) = a^2 * b^2 = a\varphi * b\varphi$;
3. If $a^2 = b^2$, then $a^2 + b^2 = 0 \Rightarrow (a+b)^2 = 0 \Rightarrow a + b = 0 \Rightarrow a = b$, φ injects;
4. For any subfield $\mathrm{GF}(\alpha_n)$, consider $\varphi_n : (\mathrm{GF}(\alpha_n), +, *) \to (\mathrm{GF}(\alpha_n), +, *); a \mapsto a^2$. The cardinality of the domain and codomain is $|\mathrm{GF}(\alpha_n)| = 2^{2^n} < \infty$. Since φ_n injects, it also surjects. Thus φ surjects.□

The automorphism φ of **N** is called the *Frobenius automorphism.*

Let K be a field, and let A be a finite-dimensional algebra over K. Let t be an element of A with characteristic polynomial $p(x)$. The *trace* $\mathrm{Tr}_K(t)$ of t over K is the negative of the coefficient of $x^{(deg\ p)-1}$ in $p(x)$. Now, let K be $\mathrm{GF}(\alpha_{n-1})$ and A be $\mathrm{GF}(\alpha_n)$. For $a \in \mathrm{GF}(\alpha_n)$, we can write $a = a_1 * \alpha_{n-1} + a_2$ with $a_i \in [0, \alpha_{n-1})$. Now $a^2 = (a_1 * \alpha_{n-1} + a_2)^2 = a_1^2 * \alpha_{n-1}^2 + a_2^2 = a_1^2 * (\alpha_{n-1} + \beta_{n-1}) + a_2^2 = a_1 * (a_1 * \alpha_{n-1}) + a_1^2 * \beta_{n-1} + a_2^2 = a_1 * (a_1 * \alpha_{n-1} + a_2) + a_1 * a_2 + a_1^2 * \beta_{n-1} + a_2^2 = a_1 * a + a_1 * a_2 + a_1^2 * \beta_{n-1} + a_2^2$, so the characteristic polynomial of $a \in \mathrm{GF}(\alpha_n)$ is $x^2 + a_1 * x + a_1 * a_2 + a_1^2 * \beta_{n-1} + a_2^2$. The coefficient of x here, viz. $\mathrm{Tr}_{\alpha_{n-1}}(a)$, is a_1. Summarizing,

Lemma 3.3 [Le2] *If* $a \in \mathrm{GF}(\alpha_n)$, *and we write* $a = a_1 * \alpha_{n-1} + a_2$, *for* $0 \le a_1, a_2 < \alpha_{n-1}$, *then* $\mathrm{Tr}_{\alpha_{n-1}}(a) = a_1$.□

Lemma 3.4 *If* $x < \alpha_n$, *then* $x\varphi^{2^n} = x^{\alpha_n} = x$.

PROOF. If $x < \alpha_n$, then $x \in \mathrm{GF}(\alpha_n)$. Certainly, $0\varphi^{2^n} = 0^{\alpha_n} = 0$. Otherwise, x is an element of the cyclic group $(\mathrm{GF}(\alpha_n)^*, *, 1)$ of order $\alpha_n - 1$. So $x\varphi^{2^n} = x^{\alpha_n} = x$, as required. □

Lemma 3.5 $\beta_n = 2^{2^n-1}$.

PROOF. One has $\beta_n = \prod_{i=0}^{n-1} \alpha_i = 2^{2^0} * 2^{2^1} * \ldots * 2^{2^{n-1}} = 2^{2^0+2^1+\ldots+2^{n-1}} = 2^{\frac{2^n-1}{2-1}} = 2^{2^n-1}$.□

Lemma 3.6 $\beta_n = \beta_{n-1} * \alpha_{n-1}$.

PROOF. $\beta_n = 2^{2^n-1} = 2^{2^{n-1}-(-2^{n-1})-1} = 2^{2^{n-1}+(2^{n-1}-1)} = 2^{2^{n-1}} * 2^{(2^{n-1}-1)} = \alpha_{n-1} * \beta_{n-1}$.□

Lemma 3.7

$$\alpha_n\varphi^k = \alpha_n + \sum_{i=0}^{k-1} \beta_n\varphi^i \tag{3.6}$$

for $n \geq 0$ *and* $k \geq 1$.

PROOF. By induction on k. For k = 1, (3.6) reduces to $\alpha_n\varphi = \alpha_n + \beta_n$, which holds by (3.5). Now assume (3.6) is true for $m < k$. Then $\alpha_n\varphi^k = (\alpha_n + \beta_n)\varphi^{k-1} = \alpha_n\varphi^{k-1} + \beta_n\varphi^{k-1} = (\alpha_n + \sum_{i=0}^{k-2} \beta_n\varphi^i) + \beta_n\varphi^{k-1} = \alpha_n + \sum_{i=0}^{k-1} \beta_n\varphi^i$, as required. □

Lemma 3.8 (Cf. [Co2, p.234]).

$$\alpha_n^{\alpha_n} = \alpha_n\varphi^{2^n} = \alpha_n + 1. \tag{3.7}$$

PROOF. By induction on n. If $n = 0$, then $\alpha_0 = 2^{2^0} = 2$, whence $\alpha_0^{\alpha_0} = 2^2 = 3 = 2+1 = \alpha_0+1$, and (3.7) holds. Now assume that $\alpha_k^{\alpha_k} = \alpha_k\varphi^{2^k} = \alpha_k+1$, for $k < n$. We want to show that $\alpha_n^{\alpha_n} = \alpha_n\varphi^{2^n} = \alpha_n + 1$. Note that $\alpha_n^{\alpha_n} = \alpha_n\varphi^{2^n} = \alpha_n + \sum_{i=0}^{2^n-1} \beta_n\varphi^i$, by Lemma 3.7.

Now, we need to show that $\sum_{i=0}^{2^n-1} \beta_n\varphi^i = 1$. Actually, we are going to prove

$$\sum_{i=0}^{2^m-1} \beta_m\varphi^i = 1 \tag{3.8}$$

for $m \leq n$, by induction on m. If $m = 0$, then (3.8) reduces to $2^{2^0-1} = 2^0 = 1$. Assume (3.8) is true for $m < n$. Then by Lemma 3.6, $\sum_{i=0}^{2^n-1} \beta_n\varphi^i = \sum_{i=0}^{2^n-1} (\alpha_{n-1} * \beta_{n-1})\varphi^i$

$$\begin{aligned}
&= \sum_{i=0}^{2^{n-1}-1} \alpha_{n-1}\varphi^i * \beta_{n-1}\varphi^i + \sum_{i=2^{n-1}}^{2^n-1} \alpha_{n-1}\varphi^i * \beta_{n-1}\varphi^i \\
&= \sum_{i=0}^{2^{n-1}-1} \alpha_{n-1}\varphi^i * \beta_{n-1}\varphi^i + \sum_{i=0}^{2^{n-1}-1} \alpha_{n-1}\varphi^{i+2^{n-1}} * \beta_{n-1}\varphi^{i+2^{n-1}} \\
&= \sum_{i=0}^{2^{n-1}-1} \alpha_{n-1}\varphi^i * \beta_{n-1}\varphi^i + \sum_{i=0}^{2^{n-1}-1} (\alpha_{n-1}\varphi^{2^{n-1}})\varphi^i * (\beta_{n-1}\varphi^{2^{n-1}})\varphi^i \\
&= \sum_{i=0}^{2^{n-1}-1} \alpha_{n-1}\varphi^i * \beta_{n-1}\varphi^i + \sum_{i=0}^{2^{n-1}-1} (\alpha_{n-1}+1)\varphi^i * \beta_{n-1}\varphi^i \\
&= \sum_{i=0}^{2^{n-1}-1} \alpha_{n-1}\varphi^i * \beta_{n-1}\varphi^i + \sum_{i=0}^{2^{n-1}-1} \alpha_{n-1}\varphi^i * \beta_{n-1}\varphi^i \\
&\quad + \sum_{i=0}^{2^{n-1}-1} 1\varphi^i * \beta_{n-1}\varphi^i \\
&= \sum_{i=0}^{2^{n-1}-1} \beta_{n-1}\varphi^i = 1, \text{ the third from last equality holding by Lemma 3.4.}
\end{aligned}$$

So we have proved $\sum_{i=0}^{2^n-1} \beta_n\varphi^i = 1$, and therefore the Lemma. □

Lemma 3.9 *Define* $A_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n); x \mapsto \sum_{i=0}^{2^n-1} x\varphi^i$. Then for $0 \leq x < \beta_n$.

$$A_n(x) = 0. \tag{3.9}$$

Moreover, $A_n(x) = \prod_{0 \le i < \beta_n}(x+i)$.

PROOF. First, note that A_n is linear, because of the linearity of φ. The result will be proved by induction on n. If $n = 0$, we have $A_0(x) = x = 0$, so 0 is the only root and (3.9) is true for $n = 0$. Assume $A_k(x) = \sum_{i=0}^{2^k-1} x\varphi^i = 0$, for $0 \le x < \beta_k$, and $0 \le k < n$. We want to show (3.9) is true for $k = n$. Since $[0, \beta_n) = [0, \alpha_{n-1}) \cup [\alpha_{n-1}, \beta_n)$, we have the following 2 cases:

Case(1) : x $\in$ GF(α_{n-1}). Here $A_n(x) = \sum_{i=0}^{2^n-1} x\varphi^i = \sum_{i=0}^{2^{n-1}-1} x\varphi^i + \sum_{i=2^{n-1}}^{2^n-1} x\varphi^i =$
$\sum_{i=0}^{2^{n-1}-1} x\varphi^i + \sum_{i=0}^{2^{n-1}-1} x\varphi^{i+2^{n-1}} = \sum_{i=0}^{2^{n-1}-1} x\varphi^i + \sum_{i=0}^{2^{n-1}-1} (x\varphi^{2^{n-1}})\varphi^i =$
$\sum_{i=0}^{2^{n-1}-1} x\varphi^i + \sum_{i=0}^{2^{n-1}-1} x\varphi^i = 0$, as required.

Case(2) : $x \in$ GF(α_n) — GF(α_{n-1}), and $x < \beta_n$. Note that x can be written as $x = x_1 * \alpha_{n-1} + x_2$, where $x_2 \in$ GF(α_{n-1}) and $1 \le x_1 < \beta_{n-1}$. So $A_n(x) = A_n(x_1 * \alpha_{n-1} + x_2) = A_n(x_1 * \alpha_{n-1}) + A_n(x_2) = A_n(x_1 * \alpha_{n-1})$

$$
\begin{aligned}
&= \sum_{i=0}^{2^n-1} (x_1 * \alpha_{n-1})\varphi^i \\
&= \sum_{i=0}^{2^{n-1}-1} (x_1 * \alpha_{n-1})\varphi^i + \sum_{i=2^{n-1}}^{2^n-1} (x_1 * \alpha_{n-1})\varphi^i \\
&= \sum_{i=0}^{2^{n-1}-1} (x_1 * \alpha_{n-1})\varphi^i + \sum_{i=0}^{2^{n-1}-1} (x_1 * \alpha_{n-1})\varphi^{i+2^{n-1}} \\
&= \sum_{i=0}^{2^{n-1}-1} (x_1 * \alpha_{n-1})\varphi^i + \sum_{i=0}^{2^{n-1}-1} ((x_1 * \alpha_{n-1})\varphi^{2^{n-1}})\varphi^i \\
&= \sum_{i=0}^{2^{n-1}-1} (x_1 * \alpha_{n-1})\varphi^i + \sum_{i=0}^{2^{n-1}-1} (x_1\varphi^{2^{n-1}} * \alpha_{n-1}\varphi^{2^{n-1}})\varphi^i \\
&= \sum_{i=0}^{2^{n-1}-1} (x_1 * \alpha_{n-1})\varphi^i + \sum_{i=0}^{2^{n-1}-1} (x_1 * (\alpha_{n-1}+1))\varphi^i \\
&= \sum_{i=0}^{2^{n-1}-1} (x_1 * \alpha_{n-1})\varphi^i + \sum_{i=0}^{2^{n-1}-1} (x_1 * \alpha_{n-1})\varphi^i + \sum_{i=0}^{2^{n-1}-1} x_1\varphi^i
\end{aligned}
$$

$$= \sum_{i=0}^{2^{n-1}-1} x_1\varphi^i = 0, \text{ as required to complete the proof of (3.9).}$$

Finally, since $\deg(A_n(x)) = \beta_n$ and $A_n(x) = 0$ for $0 \leq x < \beta_n$, the interval $[0, \beta_n)$ is a full set of roots of $A_n(x)$, i.e. $A_n(x) = \prod_{0 \leq i < \beta_n}(x + i)$.□

Lemma 3.10 *For $\beta_n \leq x < \alpha_n$, $A_n(x) = 1$. Moreover, $A_n(x) = 1 + \prod_{\beta_n \leq i < \alpha_n}(x+i)$.*

PROOF. First, observe that $A_n(x)$ is invariant under φ over $\mathrm{GF}(\alpha_n)$, i.e. $A_n(x)\varphi = A_n(x)^2 = A_n(x)$. So $A_n(x) = 1$ or 0, for $x \in \mathrm{GF}(\alpha_n)$. Now by Lemma 3.9, we have $A_n(x) = 0$, for $0 \leq x < \beta_n$. So for $x \in [0, \alpha_n) - [0, \beta_n)$, i.e. for $\beta_n \leq x < \alpha_n$, we have $A_n(x) = 1$. Similarly, since $\deg(A_n(x)) = \beta_n$, we have found all the roots of $A_n(x) = 1$, i.e. $A_n(x) + 1 = \prod_{\beta_n \leq i < \alpha_n}(x + i)$. Thus $A_n(x) = 1 + \prod_{\beta_n \leq i < \alpha_n}(x + i)$, as required. □

Corollary 3.11 $\prod_{1 \leq i < \beta_n} i = 1$, $\prod_{\beta_n \leq i < \alpha_n} i = 1$, *and* $\prod_{1 \leq i < \alpha_n} i = 1$.

PROOF. By Lemma 3.9, note that $x(x+1)(x+2)...(x+\beta_n - 1) = \sum_{i=0}^{2^n-1} x\varphi^i = \sum_{i=0}^{2^n-1} x^{2^i} = x + x^2 + x^4 + ... + x^{\beta_n} = x(1 + x + x^3 + ... + x^{\beta_n - 1})$. So $(x+1)(x+2)...(x+\beta_n - 1) = 1 + x + x^3 + ... + x^{\beta_n - 1}$. Since the leading coefficient on both sides is equal to 1, the product of all the roots on each side is equal to the constant term. Hence we have $\prod_{1 \leq i < \beta_n} i = 1$. Now by Lemma 3.10, note that $(x+\beta_n)(x+\beta_n+1)(x+\beta_n+2)...(x+\alpha_n-1) = 1 + \sum_{i=0}^{2^n-1} x\varphi^i = 1 + \sum_{i=0}^{2^n-1} x^{2^i} = 1 + x + x^2 + x^4 + ... + x^{\beta_n}$. So $(x+\beta_n)(x+\beta_n+1)(x+\beta_n+2)...(x+\alpha_n-1) = 1 + x + x^2 + x^4 + ... + x^{\beta_n}$. Since the leading coefficient on both sides is equal to 1, the product of all the roots on each side is equal to the constant term. Hence we have $\prod_{\beta_n \leq i < \alpha_n} i = 1$. The final equation $\prod_{1 \leq i < \alpha_n} i = 1$ follows from the previous 2 equations. □

Pascal's Triangle and the Sierpiński triangle

Table 3.2 displays the first few rows of Pascal's Triangle modulo 2, a pattern also known as the Sierpiński triangle. Reading the rows of the triangle as binary representations of positive integers, denote them by $P_0 = 1$, $P_1 = 3$, $P_3 = 5$, etc.

Lemma 3.12 *$P_{2^n} = 2^{2^n} + 1$, while $P_{2^n+i} = P_i * P_{2^n}$ for $1 \leq i < 2^n$.*

PROOF. Note that the kth row of Pascal's Triangle modulo 2 is determined by the coefficients of $(x+1)^k$, i.e. if we denote the coefficient of x^n in $(x+1)^k$ by k_n, then $P_k = \sum_{i=0}^{k} k_i * 2^i$. So to compute P_{2^n}, we expand $(x+1)^{2^n}$, which is equal to $x^{2^n} + 1$. Thus $P_{2^n} = 2^{2^n} + 1$. Now to compute P_{2^n+i} for $1 \leq i < 2^n$, we expand $(x+1)^{2^n+i}$ which is equal to $(x+1)^{2^n} * (x+1)^i = (x^{2^n}+1) * (x+1)^i = (x+1)^i * x^{2^n} + (x+1)^i$. So $P_{2^n+i} = P_i * 2^{2^n} + P_i = (2^{2^n}+1) * P_i = P_{2^n} * P_i$.□

Corollary 3.13 *For $1 \leq i \leq 2^{n-1}$,*

$$P_{2^n-i} = P_{2^{n-1}-i} * \alpha_{n-1} + P_{2^{n-1}-i}. \tag{3.10}$$

PROOF. $P_{2^n-i} = P_{(2^{n-1}-(-2^{n-1}))-i} = P_{2^{n-1}+(2^{n-1}-i)} = P_{2^{n-1}} * P_{2^{n-1}-i}$
$= P_{2^{n-1}-i} * \alpha_{n-1} + P_{2^{n-1}-i}$.□

Corollary 3.14 *For $1 \leq i \leq 2^{n-1}$,*
$P_{2^n-i}\varphi^j = P_{2^{n-1}-i}\varphi^j * \alpha_{n-1} + P_{2^{n-1}-i} * \sum_{k=0}^{j-1} \beta_{n-1}\varphi^k + P_{2^{n-1}-i}\varphi^j$.

PROOF. $P_{2^n-i}\varphi^j = (P_{2^{n-1}-i} * \alpha_{n-1} + P_{2^{n-1}-i})\varphi^j = P_{2^{n-1}-i}\varphi^j * \alpha_{n-1}\varphi^j + P_{2^{n-1}-i}\varphi^j =$
$P_{2^{n-1}-i}\varphi^j * (\alpha_{n-1} + \sum_{k=0}^{j-1} \beta_{n-1}\varphi^k) + P_{2^{n-1}-i}\varphi^j = P_{2^{n-1}-i}\varphi^j * \alpha_{n-1} + P_{2^{n-1}-i} * \sum_{k=0}^{j-1} \beta_{n-1}\varphi^k +$
$P_{2^{n-1}-i}\varphi^j$. The penultimate equality here follows by Lemma 3.7. □

Corollary 3.15 *For* $0 < k < 2^n$, *if we write* $k = \sum_{i=0}^{\infty} k_i * 2^i$, *with* $k_i \in \{0,1\}$, *then* $P_k = \prod\{P_{2^i} | k_i = 1\}$.

PROOF. Since $0 < k < 2^n$, there exists $m \leq n$ such that $2^{m-1} \leq k < 2^m$. We now prove the corollary by induction on m. If $m = 1$, then $k = 1$. So $k_0 = 1$, and $k_i = 0$ for $i \neq 0$. Then $\prod\{P_{2^i} | k_i = 1\} = P_{2^0} = P_1$, so the equality holds for $m = 1$. Now assume the equality for $2^{m-1} \leq k < 2^m$. We want to show that it holds for $2^m \leq k < 2^{m+1}$ too. If $2^m \leq k < 2^{m+1}$, then we can write $k = 2^m + a$, for some $a < 2^m$. Now we write $a = \sum_{i=0}^{\infty} a_i * 2^i$, where $a_i \in \{0,1\}$ for $i \leq m-1$, and $a_i = 0$ for $i \geq m$. So $k = \sum_{i=0}^{\infty} k_i * 2^i$ with $k_i = a_i$ for $0 \leq i \leq m-1, k_m = 1$, and $k_i = 0$ for $i > m$. By the induction hypothesis, we then have $P_a = \prod\{P_{2^i} | a_i = 1\}$, so $P_k = P_{2^m+a} = P_{2^m} * P_a = P_{2^m} * \prod\{P_{2^i} | a_i = 1\} = \prod\{P_{2^i} | k_i = 1\}$, as required. □

The transform and its inverse

In this section and the next, we show the general method for constructing the inverse f_n^{-1} of the transform matrix f_n defined in (3.11). In this section, we will show that the $(i+1, j)$-th entry in f_n^{-1} is the square of the (i,j)-th entry in f_n^{-1}, for $1 \leq i < 2^n$, $1 \leq j \leq 2^n$. Thus, for the construction of f_n^{-1}, it suffices to determine the numbers in the first row of f_n^{-1}. In the next section, we show that the numbers in the first row of f_n^{-1} turn out to be the rows of Pascal's Triangle modulo 2 (Theorem 3.34).

Let $f_n = f_n(1, 2, ..., 2^{2^n-1})$ be the $2^n \times 2^n$ matrix with entries given by

$$[f_n]_{i,j} = 2^{i-1}\varphi^{j-1}. \tag{3.11}$$

It is convenient to set up special notation for some other matrices. Let A_n be the $(2^n-1) \times (2^n-1)$ matrix with entries given by

$$[A_n]_{i,j} = 2^{j-1}\varphi^i. \tag{3.12}$$

Let B_n be the $(2^n-1) \times 1$ matrix with entries given by

$$[B_n]_{i,1} = 2^{2^n-1}\varphi^i. \tag{3.13}$$

Let X_n be the $(2^n-1) \times 1$ matrix with entries given by

$$[X_n]_{i,1} = P_{2^n-i}. \tag{3.14}$$

Let C_n be the $(2^n-1) \times 1$ matrix with entries given by

$$[C_n]_{i,1} = 2^{i-1}. \tag{3.15}$$

Let $d_{(a,b,n)}$ be the $(b-(a-1)) \times 1$ matrix with entries given by

$$[d_{(a,b,n)}]_{i,1} = \alpha_n\varphi^{a-(-i)-1}. \tag{3.16}$$

Let $D_{(a,b,n)}$ be the $(b-(a-1)) \times (b-(a-1))$ matrix with entries given by

$$[D_{(a,b,n)}]_{i,j} = [d_{(a,b,n)}]_{i,1} = \alpha_n\varphi^{a-(-i)-1}. \tag{3.17}$$

Let $\hat{f}_{i,j} = [f_n]_{(2^n-\{i\})\times(2^n-\{j\})}$ be the $(2^n-1) \times (2^n-1)$ matrix formed by dropping the i-th row and the j-th column from f_n, i.e.

$$\hat{f}_{a,b} = \begin{cases} 2^{i-1}\varphi^{j-1}, & \text{if } 1 \le i < a,\ 1 \le j < b; \\ 2^{i}\varphi^{j-1}, & \text{if } a \le i < 2^n,\ 1 \le j < b; \\ 2^{i-1}\varphi^{j}, & \text{if } 1 \le i < a,\ b \le j < 2^n; \\ 2^{i}\varphi^{j}, & \text{if } a \le i < 2^n,\ b \le j < 2^n. \end{cases} \tag{3.18}$$

Let R_a be the $(2^n-1) \times 1$ matrix with entries given by

$$[R_a]_{i,1} = a\varphi^i. \tag{3.19}$$

Let e_i be the $(2^n-1) \times 1$ column vector with entries given by

$$[e_i]_j = \begin{cases} 1, & \text{if } j = i; \\ 0, & \text{otherwise.} \end{cases} \tag{3.20}$$

Let $Q_{n,k}$ be the $(2^n-1) \times (2^n-1)$ matrix with the i-th column given by

$$= \begin{cases} e_i, & \text{if } 1 \le i < k; \\ e_{i+1}, & \text{if } k \le i < 2^n - 1; \\ e_k, & \text{if } i = 2^n - 1. \end{cases} \tag{3.21}$$

Lemma 3.16 *Let* $H_k(x_0, x_1, \ldots, x_{k-1})$

$$= \begin{bmatrix} x_0 & x_o\varphi & \ldots & x_0\varphi^{k-1} \\ x_1 & x_1\varphi & \ldots & x_1\varphi^{k-1} \\ \vdots & \vdots & \vdots & \vdots \\ x_{k-1} & x_{k-1}\varphi & \ldots & x_{k-1}\varphi^{k-1} \end{bmatrix}_{k\times k}$$

$$= \begin{bmatrix} x_0 & x_o^2 & \ldots & x_0^{2^{k-1}} \\ x_1 & x_1^2 & \ldots & x_1^{2^{k-1}} \\ \vdots & \vdots & \vdots & \vdots \\ x_{k-1} & x_{k-1}^2 & \ldots & x_{k-1}^{2^{k-1}} \end{bmatrix}_{k\times k}.$$

Then we have

$$\det(\mathrm{H_k}) = \prod_{\emptyset \neq I \subseteq \{0,1,2,..k-1\}} \sum_{i \in I} \mathrm{x_i}. \tag{3.22}$$

PROOF. First note that $\det(H_k) = \sum_j (-1)^{\sigma(j)}(x_0\varphi_{j_0})(x_1\varphi_{j_1})...(x_{k-1}\varphi_{j_{k-1}})$, where $\sigma(j)$ is the number of inversions in the permutation $j = (j_0, j_1, \ldots, j_n)$ and j varies over all $k!$ permutations of $\{0, 1, 2, \ldots, k-1\}$. So the determinant is a homogeneous polynomial with total degree

$$1 - (-2) - (-2^2) - ... - (-2^{k-1}) = \frac{2^k - 1}{2 - 1} = 2^k - 1 \tag{3.23}$$

in the variables $x_0, x_1, ... x_{k-1}$. On the other hand, consider $V = \{0, 1, ..., k-1\}$. Then for a non-empty subset I of V, $\sum_{i\in I} x_i$ is a factor of $\det(H_k)$. This is because, for $j \in V$, $\sum_{i\in I} x_i\varphi^j = (\sum_{i\in I} x_i)\varphi^j$, so if we add all the rows indexed in I together, we get a new row which has $(\sum_{i\in I} x_i)\varphi^j$ in the j-th entry. So these entries have the common factor $\sum_{i\in I} x_i$. And this common factor is also a factor of $\det(H_k)$. Moreover, since V has $2^k - 1$ nonempty subsets, we already have $2^k - 1$ factors of $\det(H_k)$, and hence all the factors of $\det(H_k)$ by (3.23). This completes the proof of the lemma. □

Lemma 3.17 $\det H_k(2^0, 2^1, \ldots, 2^{k-1}) = \prod_{1\le i<2^k} i$.

PROOF. By Lemma 3.16, $\det H_k(2^0, 2^1, \ldots, 2^{k-1}) = \prod_{\emptyset\neq I\subseteq\{0,1,2,..k-1\}} \sum_{i\in I} 2^i$
$= \prod_{1\le i<2^k} i$.□

Lemma 3.18 *For all* $n \ge 0$, $\det(f_n) = 1$.

PROOF. We have $\det(f_n) = \det H_{2^n}(2^0, 2^1, \ldots, 2^{k-1}) = \prod_{1\le i<2^{2^n}} i = 1$. The last equality here holds by Corollary 3.11. □

Lemma 3.19 $[f_n^{-1}]_{i,j} = \det(\hat{f}_{j,i})$.

PROOF. We have $[f_n^{-1}]_{i,j} = \det^{-1}(f_n) * \det([f_n]_{(2^n-\{j\})\times(2^n-\{i\})}) = 1*$ $\det([f_n]_{(2^n-\{j\})\times(2^n-\{i\})}) = \det([f_n]_{(2^n-\{j\})\times(2^n-\{i\})}) = \det(\hat{f}_{j,i})$ The second equality holds by Lemma 3.18, and the last by (3.18). □

Theorem 3.20 *For* $1 \le a, b \le 2^n$,

$$[f_n^{-1}]_{b,a} = [f_n^{-1}]_{1,a}\varphi^{b-1}. \tag{3.24}$$

PROOF. First, by Lemma 3.19, we have $[f_n^{-1}]_{1,a} = \det(\hat{f}_{a,1})$, $[f_n^{-1}]_{1,a}\varphi^{b-1}$ $= \det(\hat{f}_{a,1}\varphi^{b-1})$, and $[f_n^{-1}]_{b,a} = \det(\hat{f}_{a,b})$. Now

$$\hat{f}_{a,1} = \begin{cases} 2^{i-1}\varphi^j, & \text{if } 1 \le i < a,\ 1 \le j < 2^n; \\ 2^i\varphi^j, & \text{if } a \le i < 2^n,\ 1 \le j < 2^n; \end{cases}$$

and by Lemma 3.4.

$$\begin{aligned} \hat{f}_{a,1}\varphi^{b-1} &= \begin{cases} 2^{i-1}\varphi^{j-(-b)-1}, & \text{if } 1 \le i < a,\ 1 \le j < 2^n; \\ 2^i\varphi^{j-(-b)-1}, & \text{if } a \le i < 2^n,\ 1 \le j < 2^n; \end{cases} \\ &= \begin{cases} 2^{i-1}\varphi^{j-(-b)-1}, & \text{if } 1 \le i < a,\ 1 \le j < 2^n - b - (-1); \\ 2^{i-1}\varphi^{j-(-b)-1-2^n}, & \text{if } 1 \le i < a,\ 2^n - b - (-1) \le j < 2^n; \\ 2^i\varphi^{j-(-b)-1}, & \text{if } a \le i < 2^n,\ 1 \le j < 2^n - b - (-1); \\ 2^i\varphi^{j-(-b)-1-2^n}, & \text{if } a \le i < 2^n,\ 2^n - b - (-1) \le j < 2^n. \end{cases} \end{aligned}$$

Now we move the first $2^n - b$ columns to the end to form a new matrix, with the same determinant. (Recall that we are working over characteristic 2.) The new matrix $\hat{f}_{a,b}$ now has the following entries:

$$\begin{cases} 2^{i-1}\varphi^j, & \text{if } 1 \le i < a,\ b \le j < 2^n; \\ 2^{i-1}\varphi^{j-1}, & \text{if } 1 \le i < a,\ 1 \le j < b; \\ 2^i\varphi^j, & \text{if } a \le i < 2^n,\ b \le j < 2^n; \\ 2^i\varphi^{j-1}, & \text{if } a \le i < 2^n,\ 1 \le j < b. \end{cases}$$

Thus we have $[f_n^{-1}]_{1,a}\varphi^{b-1} = \det(\hat{f}_{a,1}\varphi^{b-1}) = \det(\hat{f}_{a,b}) = [f_n^{-1}]_{b,a}$, completing the proof of the theorem. □

The top of the inverse matrix

Theorem 3.20 shows that, in order to construct the inverse matrix f_n^{-1} of f_n, it remains to determine the first row. The goal of the current section, Theorem 3.34 below, identifies the first row of f_n^{-1} as $(P_{2^n-1}, ..., P_1, P_0)$. The proof of Theorem 3.34 requires a chain of auxiliary Lemmas, formulated using the notation (3.12)-(3.21).

Lemma 3.21 $\det(\hat{f}_{2^n,1}) = 1$.

PROOF. By (3.18), we have $[\hat{f}_{2^n,1}]_{i,j} = 2^{i-1}\varphi^j$, for $1 \le i, j < 2^n$.
So $\hat{f}_{2^n,1} = H_{2^n-1}(2^0\varphi, 2^1\varphi, \ldots, 2^{2^n-2}\varphi)$. Hence $\det(\hat{f}_{2^n,1})$
$= \det H_{2^n-1}(2^0\varphi, 2^1\varphi, \ldots, 2^{2^n-2}\varphi) = (\det H_{2^n-1}(2^0, 2^1, \ldots, 2^{2^n-2}))\varphi$
$= (\prod_{1 \le i < 2^{2^n-1}} i)\varphi = 1\varphi = 1$. The penultimate equality holds by Lemma 3.17, and the last by Corollary 3.11.□

Lemma 3.22 $\det(A_n) = 1$.

PROOF. By (3.12), we have that A_n^t is the $(2^n - 1) \times (2^n - 1)$ matrix with $[A_n^t]_{i,j} = 2^{i-1}\varphi^j$, and hence is equal to $\hat{f}_{2^n,1}$ by (3.18). So by Lemma 3.21, $\det(A_n) = \det(A_n^t) = \det(\hat{f}_{2^n,1}) = 1$.□

Lemma 3.23

$$\textit{Let } M_n = \begin{bmatrix} C_n^t & 2^{2^n-1} \\ A_n & B_n \end{bmatrix}_{2^n \times 2^n} . \quad \textit{Then } \mathrm{detM_n} = 1.$$

PROOF. Note M_n is the $2^n \times 2^n$ matrix with $[M_n]_{i,j} = 2^{j-1}\varphi^{i-1}$. So by (3.11) and Lemma 3.18, we have $\det M_n = \det(f_n^t) = \det(f_n) = 1$.□

Denote the *Hadamard product* of two $k \times l$ matrices E, F by $E \circ F$. Thus $[E \circ F]_{i,j} = [E_{i,j}F_{i,j}]$, for $1 \le i \le k, 1 \le j \le l$.

Lemma 3.24

$$A_{n+1} = \begin{bmatrix} A_n & B_n & A_n \circ D_{(1,2^n-1,n)} \\ C_n^t & \beta_n & (\alpha_n + 1) * C_n^t \\ A_n & B_n & A_n \circ D_{(2^n+1,2^{n+1}-1,n)} \end{bmatrix}_{(2^{n+1}-1)\times(2^{n+1}-1)} .$$

PROOF. By (3.13), A_{n+1} is the $(2^{n+1}-1) \times (2^{n+1}-1)$ matrix with $[A_{n+1}]_{i,j} = 2^{j-1}\varphi^i$. We need to verify the following 9 equations:

$$\mathbf{A_1} \equiv [A_{n+1}]_{(1,2^n-1)\times(1,2^n-1)} = A_n. \tag{3.25}$$

$$\mathbf{A_2} \equiv [A_{n+1}]_{(1,2^n-1)\times\{2^n\}} = B_n. \tag{3.26}$$

$$\mathbf{A_3} \equiv [A_{n+1}]_{(1,2^n-1)\times(2^n+1,2^{n+1}-1)} = A_n \circ D_{(1,2^n-1,n)}. \tag{3.27}$$

$$\mathbf{A_4} \equiv [A_{n+1}]_{\{2^n\}\times(1,2^n-1)} = C_n^t. \tag{3.28}$$

$$\mathbf{A_5} \equiv [A_{n+1}]_{\{2^n\}\times\{2^n\}} = \beta_n. \tag{3.29}$$

$$\mathbf{A_6} \equiv [A_{n+1}]_{\{2^n\}\times(2^n+1,2^{n+1}-1)} = (\alpha_n + 1) * C_n^t. \tag{3.30}$$

$$\mathbf{A_7} \equiv [A_{n+1}]_{(2^n+1,2^{n+1}-1)\times(1,2^n-1)} = A_n. \tag{3.31}$$

$$\mathbf{A_8} \equiv [A_{n+1}]_{(2^n+1,2^{n+1}-1)\times\{2^n\}} = B_n. \tag{3.32}$$

$$\mathbf{A_9} \equiv [A_{n+1}]_{(2^n+1,2^{n+1}-1)\times(2^n+1,2^{n+1}-1)} = A_n \circ D_{(2^n+1,2^{n+1}-1,n)}. \tag{3.33}$$

Verification of (3.25):

By definition, $\mathbf{A_1}$ is the $(2^n-1)\times(2^n-1)$ matrix with

$[\mathbf{A_1}]_{i,j} = 2^{j-1}\varphi^i$, $1 \le i,\ j \le 2^n - 1$. But this is just the matrix A_n.

Verification of (3.26):

By definition, $\mathbf{A_2}$ is the $(2^n-1)\times 1$ matrix with

$[\mathbf{A_2}]_{i,1} = 2^{2^n-1}\varphi^i$, $1 \le i \le 2^n - 1$. But this is just the matrix B_n.

Verification of (3.27):

By definition, $\mathbf{A_3}$ has coefficients as follows, for $1 \le i,\ j \le 2^n - 1$:

$[\mathbf{A_3}]_{i,j} = 2^{(2^n+j)-1}\varphi^i = 2^{2^n+(j-1)}\varphi^i = (2^{2^n} * 2^{j-1})\varphi^i = 2^{2^n}\varphi^i * 2^{j-1}\varphi^i = \alpha_n\varphi^i * [A_n]_{i,j} =$

$[D_{1,2^n-1,n}]_{i,j} * [A_n]_{i,j} = [A_n]_{i,j} * [D_{1,2^n-1,n}]_{i,j} = [A_n \circ D_{(1,2^n-1,n)}]_{i,j}$. The prepenultimate equation holds by (3.17) with $a = 1,\ b = 2^n - 1$.

Verification of (3.28):

By definition, $\mathbf{A_4}$ has coefficients as follows, for $1 \le j \le 2^n - 1$:

$[\mathbf{A_4}]_{1,j} = 2^{j-1}\varphi^{2^n} = 2^{j-1} = [C_n]_{j,1}$. So $\mathbf{A_4} = C_n^t$.

Verification of (3.29):

By definition, $\mathbf{A_5}$ is the 1×1 matrix with $[\mathbf{A_5}]_{1,1} = 2^{2^n-1}\varphi^{2^n} = 2^{2^n-1}$.

Verification of (3.30):

By definition, $\mathbf{A_6}$ has coefficients as follows, for $1 \leq i \leq 2^n - 1$:

$[\mathbf{A_6}]_{1,j} = 2^{(2^n+j)-1}\varphi^{2^n} = 2^{2^n+(j-1)}\varphi^{2^n} = (2^{2^n} * 2^{j-1})\varphi^{2^n} = 2^{2^n}\varphi^{2^n} * 2^{j-1}\varphi^{2^n} = (\alpha_n + 1) * 2^{j-1} = (\alpha_n + 1) * [C_n]_{j,1}$ So $\mathbf{A_6} = (\alpha_n + 1) * C_n^t$.

Verification of (3.31):

By definition, $\mathbf{A_7}$ has coefficients as follows, for $1 \leq i,\ j \leq 2^n - 1$:

$[\mathbf{A_7}]_{i,j} = 2^{j-1}\varphi^{(2^n+i)} = (2^{j-1}\varphi^{2^n})\varphi^i = 2^{j-1}\varphi^i = [A_n]_{i,j}$

Verification of (3.32):

By definition, $\mathbf{A_8}$ has coefficients as follows, for $1 \leq i \leq 2^n - 1$:

$[\mathbf{A_8}]_{i,1} = 2^{2^n-1}\varphi^{(2^n+i)} = (2^{2^n-1}\varphi^{2^n})\varphi^i = 2^{2^n-1}\varphi^i = [B_n]_{i,1}$

Verification of (3.33):

By definition, $\mathbf{A_9}$ has coefficients as follows, for $1 \leq i,\ j \leq 2^n - 1$:

$[\mathbf{A_9}]_{i,j} = 2^{(2^n+j)-1}\varphi^{2^n+i},\ 1 \leq i,\ j \leq 2^n - 1.$

$= 2^{2^n+(j-1)}\varphi^{2^n+i} = (2^{2^n} * 2^{j-1})\varphi^{2^n+i} = 2^{2^n}\varphi^{2^n+i} * 2^{j-1}\varphi^{2^n+i}$

$= \alpha_n\varphi^{2^n+i} * (2^{j-1}\varphi^{2^n})\varphi^i$

$= \alpha_n\varphi^{2^n+i} * 2^{j-1}\varphi^i = [D_{2^n-1,2^{n+1}-1,n}]_{i,j} * [A_n]_{i,j}$

$= [A_n]_{i,j} * [D_{2^n-1,2^{n+1}-1,n}]_{i,j}$

$= [A_n \circ D_{(2^n-1,2^{n+1}-1,n)}]_{i,j}$. The prepenultimate equation holds by (3.17) with $a = 1,\ b = 2^n - 1$ and (3.12). □

Lemma 3.25

$$X_{n+1} = \begin{bmatrix} X_n * (2^{2^n} + 1) \\ 2^{2^n} + 1 \\ X_n \end{bmatrix}_{(2^{n+1}-1)\times 1}.$$

PROOF. By (3.14), X_{n+1} is the $(2^{n+1}-1)\times 1$ matrix with $[X_{n+1}]_{i,1} = P_{2^{n+1}-i}$.
We need to verify the following 3 equations:

$$\mathbf{X_1} \equiv [X_{n+1}]_{(1,2^n-1)\times 1} = X_n * (2^{2^n}+1). \tag{3.34}$$

$$\mathbf{X_2} \equiv [X_{n+1}]_{\{2^n\}\times 1} = 2^{2^n}+1. \tag{3.35}$$

$$\mathbf{X_3} \equiv [X_{n+1}]_{(2^n+1,2^{n+1}-1)\times 1} = X_n. \tag{3.36}$$

Verification of (3.34):

By definition, $\mathbf{X_1}$ has coefficients as follows, for $1 \le i \le 2^n - 1$:

$[\mathbf{X_1}]_{i,1} = P_{2^{n+1}-i} = P_{(2^n-(-2^n))-i} = P_{2^n+(2^n-i)} = P_{2^n} * P_{2^n-i}$

$= (2^{2^n}+1) * [X_n]_{i,1} = [X_n]_{i,1} * (2^{2^n}+1)$. So $\mathbf{X_1} = X_n * (2^{2^n}+1)$.

Verification of (3.35):

By definition, $\mathbf{X_2}$ is the 1×1 matrix with $[\mathbf{X_2}]_{1,1} = P_{2^{n+1}-2^n} = P_{(2^n-(-2^n))-2^n}$

$= P_{2^n} = 2^{2^n}+1$. Verification of (3.36):

By definition, $\mathbf{X_3}$ has coefficients as follows, for $1 \le i \le 2^n - 1$:

$[\mathbf{X_3}]_{i,1} = P_{2^{n+1}-(i+2^n)} = P_{(2^n-(-2^n))-(i+2^n)} = P_{2^n-i} = [X_n]_{i,1}$.□

Lemma 3.26 *If* $A_n * X_n = B_n$, *then*

$(A_n \circ D_{(a,(2^n-2)-(-a),n)}) * X_n = B_n \circ d_{(a,(2^n-2)-(-a),n)}$.

PROOF. $(A_n \circ D_{(a,(2^n-2)-(-a),n)}) * X_n$ has coefficients as follows, for $1 \le i \le 2^n - 1$:

$[(A_n \circ D_{(a,(2^n-2)-(-a),n)}) * X_n]_{i,1}$

$$= \sum_{1\le j\le 2^n-1} [A_n \circ D_{(a,(2^n-2)-(-a),n)}]_{i,j} * [X_n]_{j,1}$$

$$
\begin{aligned}
&= \sum_{1\le j\le 2^n-1} ([A_n]_{i,j} * [D_{(a,(2^n-2)-(-a),n)}]_{i,j}) * [X_n]_{j,1}) \\
&= \sum_{1\le j\le 2^n-1} ([A_n]_{i,j} * [X_n]_{j,1}) * [D_{(a,(2^n-2)-(-a),n)}]_{i,j} \\
&= \sum_{1\le j\le 2^n-1} ([A_n]_{i,j} * [X_n]_{j,1}) * [d_{(a,(2^n-2)-(-a),n)}]_{i,1} \\
&= [d_{(a,(2^n-2)-(-a),n)}]_{i,1} * \sum_{1\le j\le 2^n-1} [A_n]_{i,j} * [X_n]_{j,1} \\
&= [d_{(a,(2^n-2)-(-a),n)}]_{i,1} * [B_n]_{i,1} \quad \text{(by hypothesis)} \\
&= [B_n]_{i,1} * [d_{(a,(2^n-2)-(-a),n)}]_{i,1} \\
&= [B_n \circ d_{(a,(2^n-2)-(-a),n)}]_{i,1}.\square
\end{aligned}
$$

Lemma 3.27 *If* $A_n * X_n = B_n$, *then* $C_n^t * X_n = 2^{2^n-1} + 1$.

PROOF. Recall the matrix M_n of Lemma 3.18. By elementary column operations, when we add the elements of the first $2^n - 1$ columns of M_n multiplied by X_n to the last column of M_n, we have a new matrix with the same determinant. Thus we have

$$
\begin{aligned}
1 &= \det \begin{bmatrix} C_n^t & 2^{2^n-1} + C_n^t * X_n \\ A_n & B_n + A_n * X_n \end{bmatrix}_{2^n \times 2^n} \\
&= \det \begin{bmatrix} C_n^t & 2^{2^n-1} + C_n^t * X_n \\ A_n & B_n + B_n \end{bmatrix}_{2^n \times 2^n} \\
&= \det \begin{bmatrix} C_n^t & 2^{2^n-1} + C_n^t * X_n \\ A_n & 0_{(2^n-1)\times 1} \end{bmatrix}_{2^n \times 2^n}.
\end{aligned}
$$

Now expanding the determinant of the matrix by the last column, we get $1 = (2^{2^n-1} + C_n^t * X_n) * \det(A_n)$. By Lemma 3.22, we thus have $2^{2^n-1} + C_n^t * X_n = 1$, i.e. $C_n^t * X_n = 2^{2^n-1} + 1$. $\square$

Lemma 3.28 *If* $A_n * X_n = B_n$, *then*

$$A_{n+1} * X_{n+1} = \begin{bmatrix} B_n \circ d_{(1,2^n-1,n)} \\ (\alpha_n + 1) * 2^{2^n-1} \\ B_n \circ d_{(2^n+1,2^{n+1}-1,n)} \end{bmatrix}_{(2^{n+1}-1)\times 1}.$$

PROOF. By Lemma 3.24 and Lemma 3.25, we have $A_{n+1} * X_{n+1}$

$$= \begin{bmatrix} A_n * X_n * (2^{2^n}+1) + B_n * (2^{2^n}+1) + (A_n \circ D_{(1,2^n-1,n)} * X_n \\ C_n^t * X_n * (2^{2^n}+1) + 2^{2^n-1} * (2^{2^n}+1) + \alpha_n^{\alpha_n} * C_n^t * X_n \\ A_n * X_n * (2^{2^n}+1) + B_n * (2^{2^n}+1) + (A_n \circ D_{(2^n+1,2^{n+1}-1,n)}) * X_n \end{bmatrix}.$$

To prove the lemma, we need to verify the following 3 equations:

$$\begin{aligned} & A_n * X_n * (2^{2^n}+1) + B_n * (2^{2^n}+1) + (A_n \circ D_{(1,2^n-1,n)} * X_n \\ = \; & B_n \circ d_{(1,2^n-1,n)}; \end{aligned} \tag{3.37}$$

$$\begin{aligned} & C_n^t * X_n * (2^{2^n}+1) + 2^{2^n-1} * (2^{2^n}+1) + \alpha_n^{\alpha_n} * C_n^t * X_n \\ = \; & (\alpha_n + 1) * 2^{2^n-1}; \end{aligned} \tag{3.38}$$

$$\begin{aligned} & A_n * X_n * (2^{2^n}+1) + B_n * (2^{2^n}+1) + (A_n \circ D_{(2^n+1,2^{n+1}-1,n)}) * X_n \\ = \; & B_n \circ d_{(2^n+1,2^{n+1}-1,n)}. \end{aligned} \tag{3.39}$$

Verification of 3.37:

$$A_n * X_n * (2^{2^n}+1) + B_n * (2^{2^n}+1) + (A_n \circ D_{(1,2^n-1,n)}) * X_n$$

$$= (A_n * X_n + B_n) * (2^{2^n}+1) + (A_n \circ D_{(1,2^n-1,n)}) * X_n$$

(by combining the first 2 terms)

$= (A_n \circ D_{(1,2^n-1,n)}) * X_n$ (by hypothesis)

$= B_n \circ d_{(1,2^n-1,n)}$ (by Lemma 3.26 with $a = 1$).

Verification of 3.38:

$C_n^t * X_n * (2^{2^n} + 1) + 2^{2^n-1} * (2^{2^n} + 1) + \alpha_n^{\alpha_n} * C_n^t * X_n$

$= (2^{2^n-1} + 1) * (2^{2^n} + 1) + 2^{2^n-1} * (2^{2^n} + 1) + \alpha_n^{\alpha_n} * (2^{2^n-1} + 1)$

(by Lemma 3.27)

$= (2^{2^n} + 1) + \alpha_n^{\alpha_n} * (2^{2^n-1} + 1)$ (by combining the first 2 terms)

$= \alpha_n + 1 + \alpha_n^{\alpha_n} * (2^{2^n-1} + 1)$

$= \alpha_n + 1 + (\alpha_n + 1) * (2^{2^n-1} + 1)$ (by Lemma 3.8)

$= (\alpha_n + 1) * 2^{2^n-1}$.

Verification of 3.39:

$A_n * X_n * (2^{2^n} + 1) + B_n * (2^{2^n} + 1) + (A_n \circ D_{(2^n+1,2^{n+1}-1,n)} * X_n$

$= (A_n * X_n + B_n) * (2^{2^n} + 1) + (A_n \circ D_{(2^n+1,2^{n+1}-1,n)} * X_n$

(by combining the first 2 terms)

$= (A_n \circ D_{(2^n+1,2^{n+1}-1,n)} * X_n$ (by hypothesis)

$= B_n \circ d_{(2^n+1,2^{n+1}-1,n)} * X_n$ (by Lemma 3.26).□

Lemma 3.29

$$B_{n+1} = \begin{bmatrix} B_n \circ d_{(1,2^n-1,n)} \\ (\alpha_n + 1) * 2^{2^n-1} \\ B_n \circ d_{(2^n+1,2^{n+1}-1,n)} \end{bmatrix}_{(2^{n+1}-1)\times 1}.$$

PROOF. By (3.13), B_{n+1} is the $(2^{n+1}-1)\times 1$ matrix with

$[B_{n+1}]_{i,1} = 2^{2^{n+1}-1}\varphi^i$.

We need to verify the following 3 equations:

$$\mathbf{B_1} \equiv [B_{n+1}]_{(1,2^n-1)\times 1} = B_n \circ d_{(1,2^n-1,n)}. \tag{3.40}$$

$$\mathbf{B_2} \equiv [B_{n+1}]_{\{2^n\}\times 1} = (\alpha_n + 1) * 2^{2^n-1}. \tag{3.41}$$

$$\mathbf{B_3} \equiv [B_{n+1}]_{(2^n+1,2^{n+1}-1)\times 1} = B_n \circ d_{(2^n+1,2^{n+1}-1,n)}. \tag{3.42}$$

Verification of (3.40):

By definition, $\mathbf{B_1}$ has coefficients as follows, for $1 \le i \le 2^n - 1$:

$[\mathbf{B_1}]_{i,1} = 2^{2^{n+1}-1}\varphi^i = 2^{(2^n-(-2^n))-1}\varphi^i = 2^{2^n+(2^n-1)}\varphi^i = (2^{2^n} * 2^{2^n-1})\varphi^i = 2^{2^n}\varphi^i *$
$2^{2^n-1}\varphi^i = \alpha_n\varphi^i * [B_n]_{i,1} = [d_{(1,2^n-1,n)}]_{i,1} * [B_n]_{i,1} = [B_n]_{i,1} * [d_{(1,2^n-1,n)}]_{i,1} = [B_n \circ$
$d_{(1,2^n-1,n)}]_{i,1}$. The prepenultimate equation holds by (3.16) with $a = 1, b = 2^n - 1$.

Verification of (3.41):

By definition, $\mathbf{B_2}$ is the 1×1 matrix with

$[\mathbf{B_2}]_{1,1} = 2^{2^{n+1}-1}\varphi^{2^n} = 2^{(2^n-(-2^n))-1}\varphi^{2^n} = 2^{2^n+(2^n-1)}\varphi^{2^n} = (2^{2^n} * 2^{2^n-1})\varphi^{2^n} = 2^{2^n}\varphi^{2^n} *$
$2^{2^n-1}\varphi^{2^n} = (\alpha_n + 1) * 2^{2^n-1}$.

Verification of (3.42):

By definition, $\mathbf{B_3}$ has coefficients as follows, for $1 \le i \le 2^n - 1$:

$[\mathbf{B_3}]_{i,1} = 2^{2^{n+1}-1}\varphi^{2^n+i} = 2^{(2^n-(-2^n))-1}\varphi^{2^n+i} = 2^{2^n+(2^n-1)}\varphi^{2^n+i} = (2^{2^n} * 2^{2^n-1})\varphi^{2^n+i} =$
$2^{2^n}\varphi^{2^n+i} * 2^{2^n-1}\varphi^{2^n+i} = \alpha_n\varphi^{2^n+i} * (2^{2^n-1}\varphi^{2^n})\varphi^i = \alpha_n\varphi^{2^n+i} * 2^{2^n-1}\varphi^i = \alpha_n\varphi^{2^n+i} *$
$[B_n]_{i,1} = [d_{(2^n+1,2^{n+1}-1,n)}]_{i,1} * [B_n]_{i,1} = [B_n]_{i,1} * [d_{(2^n+1,2^{n+1}-1,n)}]_{i,1} = [B_n \circ d_{(2^n+1,2^{n+1}-1,n)}]_{i,1}$.
The prepenultimate equation holds by (3.16) with $a = 2^n + 1, b = 2^{n+1} - 1$. □

Lemma 3.30 $A_n * X_n = B_n$.

PROOF. By induction on n. If $n = 1$, we have $A_1 * X_1 = [1][P_1] = 1 \times 3 = 2^2 = B_1$. Assume $A_k * X_k = B_k$. We want to show $A_{k+1} * X_{k+1} = B_{k+1}$. By the induction hypothesis, Lemma 3.28 and Lemma 3.29, we have

$$A_{k+1} * X_{k+1} = \begin{bmatrix} B_k \circ d_{(1,2^k-1,k)} \\ (\alpha_k + 1) * 2^{2^k-1} \\ B_k \circ d_{(2^k+1,2^{k+1}-1,k)} \end{bmatrix}_{(2^{n+1}-1)\times 1} = B_{k+1}.$$

This completes the proof of the lemma. □

Lemma 3.31 $(A_n Q_{n,k}) * (Q_{n,k}^t X_n) = B_n$.

PROOF. $(A_n Q_{n,k}) * (Q_{n,k}^t X_n)$ has coefficients as follows, for $1 \le i \le 2^n - 1$:

$$[(A_n Q_{n,k}) * (Q_{n,k}^t X_n)]_{i,1} = \sum_{j=1}^{2^n-1} [A_n Q_{n,k}]_{i,j} * [Q_{n,k}^t X_n]_{j,1}$$

$$\begin{aligned}
&= \sum_{j=1}^{k-1} [A_n Q_{n,k}]_{i,j} * [Q_{n,k}^t X_n]_{j,1} + \sum_{j=k}^{2^n-2} [A_n Q_{n,k}]_{i,j} * [Q_{n,k}^t X_n]_{j,1} \\
&+ [A_n Q_{n,k}]_{i,2^n-1} * [Q_{n,k}^t X_n]_{2^n-1,1} \\
&= \sum_{j=1}^{k-1} [A_n]_{i,j} * [X_n]_{j,1} + \sum_{j=k}^{2^n-2} [A_n]_{i,j+1} * [X_n]_{j+1,1} + [A_n]_{i,k} * [X_n]_{k,1} \\
&= \sum_{j=1}^{k-1} [A_n]_{i,j} * [X_n]_{j,1} + \sum_{j=k+1}^{2^n-1} [A_n]_{i,j} * [X_n]_{j,1} + [A_n]_{i,k} * [X_n]_{k,1} \\
&= \sum_{j=1}^{2^n-1} [A_n]_{i,j} * [X_n]_{j,1} = [A_n * X_n]_{i,1} = [B_n]_{i,1}.
\end{aligned}$$

Thus $(A_n Q_{n,k}) * (Q_{n,k}^t X_n) = B_n$. □

Lemma 3.32 *Let E be the $(2^n - 1) \times (2^n - 1)$ matrix with e_i as its i-th column, for $1 \le i < 2^n - 1$, and $Q_{n,k}^t X_n$ as its last column. We then have $(A_n Q_{n,k}) * E = \hat{f}_{k,1}^t$.*

PROOF. Note that $\hat{f}_{k,1}^t$ is the $(2^n-1)\times(2^n-1)$ matrix whose i-th column is

$$\begin{cases} R_{2^{i-1}} & , 1 \le i < k; \\ R_{2^i} & , k \le i \le 2^n - 1. \end{cases}$$

$A_nQ_{n,k}$ is the $(2^n-1)\times(2^n-1)$ matrix whose i-th column is

$$\begin{cases} R_{2^{i-1}} & , 1 \le i < k; \\ R_{2^i} & , k \le i < 2^n - 1; \\ R_{2^{k-1}} & , i = 2^n - 1. \end{cases}$$

So the first 2^n-2 columns of $A_nQ_{n,k}$ and $\hat{f}_{k,1}^t$ agree. Hence for $1 \le i < 2^n-1$, $(A_nQ_{n,k}) * e_i$ is equal to the i-th column of $A_nQ_{n,k}$, which is equal to the i-th column of $\hat{f}_{k,1}^t$. We also have $(A_nQ_{n,k}) * (Q_{n,k}^t X_n) = B_n$ by Lemma 3.31. Since $B_n = R_{2^{2^n-1}}$ by (3.13) and (3.19), $(A_nQ_{n,k}) * E = \hat{f}_{k,1}^t$. □

Lemma 3.33 *Let E be defined as in Lemma* 3.32. *Then* $\det(E) = P_{2^n-i}$.

PROOF. Since the i-th column of the matrix E is e_i, for $1 \le i < 2^n-1$, $\det(E) = [Q_{n,k}^t X_n]_{2^n-1,1} = P_{2^n-i}$. □

Theorem 3.34 *Let f_n be defined as in* (3.11). *Then the first row of f_n^{-1} is* $(P_{2^n-1}, \ldots, P_1, P_0)$.

PROOF. We want to show that $[f_n^{-1}]_{1,i} = P_{2^n-i}$, for $1 \le i \le 2^n$. But $[f_n^{-1}]_{1,i} = \det(\hat{f}_{i,1}) = \det(\hat{f}_{i,1}^t) = \det((A_nQ_{n,k})*E) = \det(A_nQ_{n,k})*\det(E) = \det(A_n)*\det(E) = 1 * P_{2^n-i} = P_{2^n-i}$, as required. □

Corollary 3.35 $[f_n^{-1}]_{i,j} = P_{2^n-j}\varphi^{i-1}$, *for* $1 \leq i,j \leq 2^n$.

PROOF. By Theorem 3.20 and Theorem 3.34. □

Function spaces

This section studies relationships between certain subspaces of the GF(2)-space $\prod_{n=0}^{\infty}$End GF(α_n). The subspaces are of interest in coding theory, since they contain the syndromes of binary lexicodes.

Definition 3.36 *A sequence of* GF(2)*-linear functions* $\{h_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ *is said to be* **coherent** *if there exists a* GF(2)*-linear function* $f : \mathbf{N} \to \mathbf{N}$ *such that* $\exists n.\ \forall m \geq n,\ h_m = f|_{\mathrm{GF}(\alpha_m)}$. *Let* C *denote the subset of* $\prod_{n=0}^{\infty}$End GF(α_n) *consisting of coherent sequences.*

Proposition 3.37 *The set* C *of coherent sequences forms a subspace of* $\prod_{n=0}^{\infty}$ End GF(α_n).

PROOF. First, note that the sequence of zero functions is coherent. Now let $\{h_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ and $\{k_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ be coherent sequences. To prove C is a subspace, we need to show that $\{l_n = h_n + k_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ is a coherent sequence too, since we are working over GF(2). Now we have : there exists a GF(2)-linear function $f : \mathbf{N} \to \mathbf{N}$ such that $\exists n_1.\ \forall m \geq n_1,\ h_m = f|_{\mathrm{GF}(\alpha_m)}$ and there exists a GF(2)-linear function $g : \mathbf{N} \to \mathbf{N}$ such that $\exists n_2.\ \forall m \geq n_2,\ k_m = g|_{\mathrm{GF}(\alpha_m)}$. Let $n = \max(n_1, n_2)$. Then $\forall m \geq n,\ h_m = f|_{\mathrm{GF}(\alpha_m)}$ and $k_m = g|_{\mathrm{GF}(\alpha_m)}$, so $l_m = h_m + k_m = (f+g)|_{\mathrm{GF}(\alpha_m)}$. Since $f + g : \mathbf{N} \to \mathbf{N}$ is again a linear function, the proposition is proved. □

Definition 3.38 *A sequence of* GF(2)*-linear functions* $\{h_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ *is said to be* **small** *if* $\exists n.\ \forall m \geq n,\ \mathrm{GF}(\alpha_m)h_m \subseteq \mathrm{GF}(\alpha_{m-1})$. *Let* S *denote the subset of* $\prod_{n=0}^{\infty}\mathrm{End}\ \mathrm{GF}(\alpha_n)$ *consisting of small sequences.*

Proposition 3.39 *The set* S *of small sequences forms a subspace of* $\prod_{n=0}^{\infty}$ End $\mathrm{GF}(\alpha_n)$.

PROOF. First, note that the sequence of zero functions is small. Now let $\{h_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ and $\{k_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ be small sequences. To prove S is a subspace, we need to show that $\{l_n = h_n + k_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ is a small sequence too. Now we have: $\exists n_1.\ \forall m \geq n_1, \mathrm{GF}(\alpha_m)h_m \subseteq \mathrm{GF}(\alpha_{m-1})$ and $\exists n_2.\ \forall m \geq n_2, \mathrm{GF}(\alpha_m)k_m \subseteq \mathrm{GF}(\alpha_{m-1})$. Let $n = \max(n_1, n_2)$. Then $\forall m \geq n,\ \mathrm{GF}(\alpha_m)h_m \subseteq \mathrm{GF}(\alpha_{m-1})$ and $\mathrm{GF}(\alpha_m)k_m \subseteq \mathrm{GF}(\alpha_{m-1})$, so $\mathrm{GF}(\alpha_m)(l_m) = \mathrm{GF}(\alpha_m)(h_m + k_m) \subseteq \mathrm{GF}(\alpha_{m-1})$. □

Definition 3.40 *A sequence of* GF(2)*-linear functions* $\{h_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ *is said to* **nest** *if* $\exists n.\ \forall m \geq n, \forall 0 \leq i < 2^{m-1}, \mathrm{Tr}_{\alpha_{m-1}}(\breve{h}_m(2^i)) = \mathrm{Tr}_{\alpha_{m-1}}(\breve{h}_m(2^{i+2^{m-1}})) = \breve{h}_{m-1}(2^i)$. *Let* N *denote the subset of* $\prod_{n=0}^{\infty}\mathrm{End}\ \mathrm{GF}(\alpha_n)$ *consisting of nesting sequences.*

Proposition 3.41 *The set* N *of nesting sequences forms a subspace of* $\prod_{n=0}^{\infty}$ End $\mathrm{GF}(\alpha_n)$.

PROOF. First, note that the sequence of zero functions is nested. Now let $\{h_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ and $\{k_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ be nesting sequences. To prove N is a subspace, we need to show that $\{l_n = h_n + k_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ is a nesting sequence too. Now we have : $\exists n_1.\ \forall m \geq n_1, \forall 0 \leq i < 2^{m-1}, \mathrm{Tr}_{\alpha_{m-1}}(\breve{h}_m(2^i)) =$

$\mathrm{Tr}_{\alpha_{m-1}}(\breve{h}_m(2^{i+2^{m-1}})) = \breve{h}_{m-1}(2^i)$, and $\exists n_2.\ \forall m \geq n_2, \forall 0 \leq i < 2^{m-1}, \mathrm{Tr}_{\alpha_{m-1}}(\breve{k}_m(2^i)) = \mathrm{Tr}_{\alpha_{m-1}}(\breve{k}_m(2^{i+2^{m-1}})) = \breve{h}_{m-1}(2^i)$. Let $n = \max(n_1, n_2)$. Then $\forall m \geq n,\ \forall 0 \leq i < 2^{m-1}, \mathrm{Tr}_{\alpha_{m-1}}(\breve{h}_m(2^i)) = \mathrm{Tr}_{\alpha_{m-1}}(\breve{h}_m(2^{i+2^{m-1}}))$ and $\breve{k}_{m-1}(2^i)\ \mathrm{Tr}_{\alpha_{m-1}}(\breve{k}_m(2^i)) = \mathrm{Tr}_{\alpha_{m-1}}(\breve{h}_m(2^{i+2^{m-1}})) = \breve{h}_{m-1}(2^i)$. Now $l_n = h_n + k_n$ implies $\breve{l}_n = \breve{h}_n + \breve{k}_n$. Also the trace is a linear function. So $\mathrm{Tr}_{\alpha_{m-1}}((\breve{l}_m)(2^i)) = \mathrm{Tr}_{\alpha_{m-1}}((\breve{h}_m + \breve{k}_m)(2^i)) = \mathrm{Tr}_{\alpha_{m-1}}(\breve{h}_m)(2^i)) + \mathrm{Tr}_{\alpha_{m-1}}(\breve{k}_m)(2^i)) = \mathrm{Tr}_{\alpha_{m-1}}(\breve{h}_m(2^{i+2^{m-1}})) + \mathrm{Tr}_{\alpha_{m-1}}(\breve{k}_m(2^{i+2^{m-1}})) = \mathrm{Tr}_{\alpha_{m-1}}((\breve{h}_m + \breve{k}_m)(2^{i+2^{m-1}})) = \mathrm{Tr}_{\alpha_{m-1}}(\breve{l}_m(2^{i+2^{m-1}}))$. Also, $= \breve{h}_{m-1}(2^i) + \breve{k}_{m-1}(2^i) = (\breve{k}_{m-1} + \breve{k}_{m-1})(2^i) = \breve{l}_{m-1}(2^i)$. □

Definition 3.42 *A sequence of* GF(2)*-linear functions* $\{h_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ *is said to have the* **martingale property** *if* $\exists n.\ \forall m \geq n, \forall 0 \leq i < 2^{m-1}, \breve{h}_m(2^i) + \breve{h}_m(2^{i+2^{m-1}}) = \breve{h}_{m-1}(2^i)$. *Let* M *denote the subset of* $\prod_{n=0}^{\infty}\mathrm{End}\ \mathrm{GF}(\alpha_n)$ *consisting of sequences having the martingale property.*

Proposition 3.43 *The set* M *of sequences with the martingale property forms a subspace of* $\prod_{n=0}^{\infty}$ End $\mathrm{GF}(\alpha_n)$.

PROOF. First, note that the sequence of zero functions has the martingale property. Now let $\{h_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ and $\{k_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ be sequences with the martingale property. To prove M is a subspace, we need to show that $\{l_n = h_n + k_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ is a sequence with the martingale property too. Now we have : $\exists n_1.\ \forall m \geq n_1, \forall 0 \leq i < 2^{m-1}, \breve{h}_m(2^i) + \breve{h}_m(2^{i+2^{m-1}}) = \breve{h}_{m-1}(2^i)$ and $\exists n_2.\ \forall m \geq n_2, \forall 0 \leq i < 2^{m-1}, \breve{k}_m(2^i) + \breve{k}_m(2^{i+2^{m-1}}) = \breve{k}_{m-1}(2^i)$. Let $n = \max(n_1, n_2)$. Then $\forall m \geq n,\ \forall 0 \leq i < 2^{m-1}, \breve{h}_m(2^i) + \breve{h}_m(2^{i+2^{m-1}}) = \breve{h}_{m-1}(2^i)$ and $\breve{k}_m(2^i) + \breve{k}_m(2^{i+2^{m-1}}) = \breve{k}_{m-1}(2^i)$, so $(\breve{l}_m)(2^i) + (\breve{l}_m)(2^{i+2^{m-1}}) = (\breve{h}_m + \breve{k}_m)(2^i) + (\breve{h}_m +$

$\breve{k}_m)(2^{i+2^{m-1}}) = \breve{h}_m(2^i) + \breve{k}_m(2^i) + \breve{h}_m(2^{i+2^{m-1}}) + \breve{k}_m(2^{i+2^{m-1}}) = \breve{h}_{m-1}(2^i) + \breve{k}_{m-1}(2^i) = \breve{l}_{m-1}(2^i)$. □

Theorem 3.44 *Coherent sequences have the martingale property : $C \subseteq M$. In other words, if $\{h_n\}$ is a sequence of linear functions with $h_n(2^i) = h_{n-1}(2^i)$, for $0 \leq i < 2^{n-1}$, then $\breve{h}_n(2^i) + \breve{h}_n(2^{i+2^{n-1}}) = \breve{h}_{n-1}(2^i)$, for $0 \leq i < 2^{n-1}$.*

PROOF. First,

$$\begin{aligned}
\breve{h}_n(2^i) &= \sum_{j=1}^{2^n} [f_n^{-1}]_{i-(-1),j} * h_n(2^{j-1}) \quad \text{(by Corollary 3.35)} \\
&= \sum_{j=1}^{2^n} P_{2^n-j}\varphi^i * h_n(2^{j-1}) \\
&= \sum_{j=1}^{2^n} P_{2^{n-1}+(2^{n-1}-j)}\varphi^i * h_n(2^{j-1}) \\
&= \sum_{j=1}^{2^n} (P_{2^{n-1}} * P_{2^{n-1}-j})\varphi^i * h_n(2^{j-1}) \\
&= \sum_{j=1}^{2^n} ((\alpha_{n-1}+1) * P_{2^{n-1}-j})\varphi^i * h_n(2^{j-1}) \\
&= \sum_{j=1}^{2^n} (\alpha_{n-1} * P_{2^{n-1}-j} + P_{2^{n-1}-j})\varphi^i * h_n(2^{j-1}).
\end{aligned}$$

And,

$\breve{h}_n(x^{2^{i+2^{n-1}}})$

$$\begin{aligned}
&= \sum_{j=1}^{2^n} [f_n^{-1}]_{(i+2^{n-1})-(-1),j} * h_n(2^{j-1}) \quad \text{(by Corollary 3.35)} \\
&= \sum_{j=1}^{2^n} P_{2^n-j}\varphi^{i+2^{n-1}} * h_n(2^{j-1}) \\
&= \sum_{j=1}^{2^n} P_{2^n-j}\varphi^{2^{n-1}+i} * h_n(2^{j-1})
\end{aligned}$$

$$= \sum_{j=1}^{2^n}(P_{2^n-j}\varphi^{2^{n-1}})\varphi^i * h_n(2^{j-1})$$

$$= \sum_{j=1}^{2^{n-1}}(P_{2^n-j}\varphi^{2^{n-1}})\varphi^i * h_n(2^{j-1}) + \sum_{j=2^{n-1}+1}^{2^n}(P_{2^n-j}\varphi^{2^{n-1}})\varphi^i * h_n(2^{j-1})$$

$$= \sum_{j=1}^{2^{n-1}}(P_{2^n-j}\varphi^{2^{n-1}})\varphi^i * h_n(2^{j-1}) + \sum_{j=2^{n-1}+1}^{2^n} P_{2^n-j}\varphi^i * h_n(2^{j-1}),$$

since $P_{2^n-j} < \alpha_{n-1}$ for $2^{n-1}+1 \le j \le 2^n$ and by Lemma 3.4.

$$= \sum_{j=1}^{2^{n-1}}(P_{2^{n-1}+(2^{n-1}-j)}\varphi^{2^{n-1}})\varphi^i * h_n(2^{j-1}) + \sum_{j=2^{n-1}+1}^{2^n} P_{2^{n-1}+(2^{n-1}-j)}\varphi^i * h_n(2^{j-1})$$

$$= \sum_{j=1}^{2^{n-1}}((P_{2^{n-1}} * P_{2^{n-1}-j})\varphi^{2^{n-1}})\varphi^i * h_n(2^{j-1}) + \sum_{j=2^{n-1}+1}^{2^n}(P_{2^{n-1}} * P_{2^{n-1}-j})\varphi^i * h_n(2^{j-1})$$

$$= \sum_{j=1}^{2^{n-1}}(((\alpha_{n-1}+1) * P_{2^{n-1}-j})\varphi^{2^{n-1}})\varphi^i * h_n(2^{j-1})$$

$$+ \sum_{j=2^{n-1}+1}^{2^n}((\alpha_{n-1}+1) * P_{2^{n-1}-j}))\varphi^i * h_n(2^{j-1})$$

$$= \sum_{j=1}^{2^{n-1}}((\alpha_{n-1}\varphi^{2^{n-1}} + 1\varphi^{2^{n-1}}) * P_{2^{n-1}-j}\varphi^{2^{n-1}})\varphi^i * h_n(2^{j-1})$$

$$+ \sum_{j=2^{n-1}+1}^{2^n}((\alpha_{n-1}+1) * P_{2^{n-1}-j}))\varphi^i * h_n(2^{j-1})$$

$$= \sum_{j=1}^{2^{n-1}}(((\alpha_{n-1}+1)+1) * P_{2^{n-1}-j})\varphi^i * h_n(2^{j-1})$$

$$+ \sum_{j=2^{n-1}+1}^{2^n}(\alpha_{n-1} * P_{2^{n-1}-j} + P_{2^{n-1}-j})\varphi^i * h_n(2^{j-1}) \quad (\text{ by Lemma 3.8 and}$$

Lemma 3.4 with $P_{2^{n-1}-j} < \alpha_{n-1}$, for $1 \le j \le 2^{n-1}$.)

$$= \sum_{j=1}^{2^{n-1}}(\alpha_{n-1} * P_{2^{n-1}-j})\varphi^i * h_n(2^{j-1})$$

$$+ \sum_{j=2^{n-1}+1}^{2^n}(\alpha_{n-1} * P_{2^{n-1}-j} + P_{2^{n-1}-j})\varphi^i * h_n(2^{j-1})$$

So,

$$\breve{h}_n(2^i) + \breve{h}_n(2^{i+2^{n-1}})$$

$$= \sum_{j=1}^{2^n}(\alpha_{n-1} * P_{2^{n-1}-j} + P_{2^{n-1}-j})\varphi^i * h_n(2^{j-1}) + \sum_{j=1}^{2^{n-1}}(\alpha_{n-1} * P_{2^{n-1}-j})\varphi^i * h_n(2^{j-1})$$

$$+ \sum_{j=2^{n-1}+1}^{2^n}(\alpha_{n-1} * P_{2^{n-1}-j} + P_{2^{n-1}-j})\varphi^i * h_n(2^{j-1})$$

$$= \sum_{j=1}^{2^{n-1}}(\alpha_{n-1} * P_{2^{n-1}-j} + P_{2^{n-1}-j})\varphi^i * h_n(2^{j-1})$$

$$+ \sum_{j=2^{n-1}+1}^{2^n}(\alpha_{n-1} * P_{2^{n-1}-j} + P_{2^{n-1}-j})\varphi^i * h_n(2^{j-1}) + \sum_{j=1}^{2^{n-1}}(\alpha_{n-1} * P_{2^{n-1}-j})\varphi^i$$

$$*h_n(2^{j-1}) + \sum_{j=2^{n-1}+1}^{2^n}(\alpha_{n-1} * P_{2^{n-1}-j} + P_{2^{n-1}-j})\varphi^i * h_n(2^{j-1})$$

$$= \sum_{j=1}^{2^{n-1}}(\alpha_{n-1} * P_{2^{n-1}-j} + P_{2^{n-1}-j})\varphi^i * h_n(2^{j-1}) + \sum_{j=1}^{2^{n-1}}(\alpha_{n-1} * P_{2^{n-1}-j})\varphi^i * h_n(2^{j-1})$$

$$= \sum_{j=1}^{2^{n-1}} P_{2^{n-1}-j}\varphi^i * h_n(2^{j-1})$$

$$= \sum_{j=1}^{2^{n-1}} P_{2^{n-1}-j}\varphi^i * h_{n-1}(2^{j-1}) \quad (\text{ by hypothesis})$$

$$= \sum_{j=1}^{2^{n-1}} [f_{n-1}]_{i+1,j} * h_{n-1}(2^{j-1}) \quad (\text{ by Corollary 3.35})$$

$$= \breve{h}_{n-1}(2^i), \text{ as required.}\square$$

Theorem 3.45 *The martingale property implies the coherence property: $M \subseteq C$. In other words, if a sequence $\{h_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ of $\mathrm{GF}(2)$-linear functions satisfies $\breve{h}_n(2^i)+\breve{h}_n(2^{i+2^{n-1}}) = \breve{h}_{n-1}(2^i)$, for $0 \le i < 2^{n-1}$, then $h_n(2^i) = h_{n-1}(2^i)$, for $0 \le i < 2^{n-1}$.*

PROOF. We want to show $h_n(2^i) = h_{n-1}(2^i)$, for $0 \leq i < 2^{n-1}$. For $0 \leq i < 2^{n-1}$, we have

$$\begin{aligned}
h_n(2^i) &= \sum_{j=0}^{2^n-1} [f_n]_{i+1,j+1} * \breve{h}_n(2^j) \\
&= \sum_{j=0}^{2^n-1} 2^i\varphi^j * \breve{h}_n(2^j) \quad \text{(by Equation 3.11)} \\
&= \sum_{j=0}^{2^{n-1}-1} 2^i\varphi^j * \breve{h}_n(2^j) + \sum_{j=2^{n-1}}^{2^n-1} 2^i\varphi^j * \breve{h}_n(2^j) \\
&= \sum_{j=0}^{2^{n-1}-1} 2^i\varphi^j * \breve{h}_n(2^j) + \sum_{j=0}^{2^{n-1}-1} 2^i\varphi^{2^{n-1}+j} * \breve{h}_n(2^{2^{n-1}+j}) \\
&\quad \text{(by change of indices)} \\
&= \sum_{j=0}^{2^{n-1}-1} 2^i\varphi^j * \breve{h}_n(2^j) + \sum_{j=0}^{2^{n-1}-1} (2^i\varphi^{2^{n-1}})\varphi^j * \breve{h}_n(2^{2^{n-1}+j}) \\
&= \sum_{j=0}^{2^{n-1}-1} 2^i\varphi^j * \breve{h}_n(2^j) + \sum_{j=0}^{2^{n-1}-1} 2^i\varphi^j * \breve{h}_n(2^{2^{n-1}+j}) \\
&\quad \text{(since } 2^i < \alpha_{n-1}, \text{ for } 0 \leq i < 2^{n-1}) \\
&= \sum_{j=0}^{2^{n-1}-1} 2^i\varphi^j * (\breve{h}_n(2^j) + \breve{h}_n(2^{2^{n-1}+j})) \\
&= \sum_{j=0}^{2^{n-1}-1} 2^i\varphi^j * \breve{h}_{n-1}(2^j) \quad \text{(by hypothesis)} \\
&= \sum_{j=0}^{2^{n-1}-1} [f_{n-1}]_{i+1,j+1} * \breve{h}_{n-1}(2^j) \quad \text{(by Equation 3.11)} \\
&= h_{n-1}(2^i). \square
\end{aligned}$$

Corollary 3.46 *The martingale property is equivalent to coherence.* □

We now provide some examples demonstrating the independence of the function spaces introduced in this section.

Example 3.47 *A coherent sequence need not nest, i.e.* $C \not\subseteq N$.

Let

$$h_n(2^i) = \begin{cases} \beta_k & ,\text{if } i = 2^k - 1, 1 \le k \le n; \\ 0 & , \text{otherwise.} \end{cases}$$

for all n. Then $\{h_n\}$ is a coherent sequence. But $\breve{h}_n(2^0) = \sum_{k=1}^{n} \beta_k P_{2^n-2^k}$ and

$$\begin{aligned}
\breve{h}_{n+1}(2^0) &= \sum_{k=1}^{n+1} \beta_k * P_{2^{n+1}-2^k} \\
&= \sum_{k=1}^{n} \beta_k * P_{2^{n+1}-2^k} + \beta_{n+1} P_0 \\
&= \sum_{k=1}^{n} \beta_k * P_{2^n+(2^n-2^k)} + \beta_{n+1} \\
&= \sum_{k=1}^{n} \beta_k * (P_{2^n} * P_{2^n-2^k}) + \beta_{n+1} \\
&= P_{2^n} * \sum_{k=1}^{n} \beta_k * P_{2^n-2^k} + \beta_{n+1} \\
&= (\alpha_n + 1) * \sum_{k=1}^{n} \beta_k * P_{2^n-2^k} + \beta_{n+1} \\
&= (\alpha_n + 1) * \sum_{k=1}^{n} \beta_k * P_{2^n-2^k} + \alpha_n * \beta_n \\
&= \alpha_n * (\beta_n + \sum_{k=1}^{n} \beta_k * P_{2^n-2^k}) + \sum_{k=1}^{n} \beta_k * P_{2^n-2^k} \\
&= \alpha_n * (\beta_n + \breve{h}_n(2^0)) + \breve{h}_n(2^0) \\
&= (\beta_n + \breve{h}_n(2^0)) * \alpha_n + \breve{h}_n(2^0).
\end{aligned}$$

Since $\beta_n + \breve{h}_n(2^0)$ is not equal to $\breve{h}_n(2^0)$ and $\breve{h}_n(2^0) < \alpha_n$, we conclude that $\{h_n\}$ is not nesting.

Example 3.48 *A small sequence need not nest, i.e.* $S \not\subseteq N$.

Let

$$h_n(2^i) = \begin{cases} 1 & ,\text{if } i = 2^n - 1; \\ 0 & , \text{otherwise,} \end{cases}$$

for all n. Then $\{h_n\}$ is small. But $\breve{h}_n(2^i) = 1$, for all n and all i, so $\{h_n\}$ is not nesting.

Example 3.49 *A small sequence need not be coherent, i.e.* $S \not\subseteq C$.

The sequence $\{h_n\}$ of Example 3.48 works here.

Example 3.50 *A nesting sequence need not be coherent, i.e.* $N \not\subseteq C$.

Let $\breve{h}_1 = \{1, 1\}$ and $\breve{h}_n(2^i) = \beta_n$, for all i and $n \geq 2$. We then have that $\{h_n\}$ is nesting. But also

$$h_n(2^i) = \begin{cases} \beta_n & \text{, if } i = 2^n - 1; \\ 0 & \text{, otherwise,} \end{cases}$$

i.e. $\{h_n\}$ is not a coherent sequence.

Example 3.51 *A nesting sequence need not be small, i.e.* $N \not\subseteq S$.

The nesting sequence $\{h_n\}$ of Example 3.50 works here, since $h_n(2^{2^n-1}) = \beta_n \notin \mathrm{GF}(\alpha_{n-1})$ for all n.

Example 3.52 *A sequence with the martingale property need not be small, i.e.* $M \not\subseteq S$.

Let $\breve{h}_n(2^0) = 1$ and $\breve{h}_n(2^i) = 0$, for $1 \leq i < 2^n$ and for all n. Then $\{h_n\}$ satisfies the martingale property, but we have $\forall n, h_n(2^{2^n-1}) = \beta_n > \alpha_{n-1}$, i.e. $\{h_n\}$ is not small.

Small, coherent sequences

This section completes the investigation of the relationship between the function spaces C, N and S by showing (Corollary 3.63) that

$$C \cap N = N \cap S = S \cap C. \tag{3.43}$$

Theorem 3.53 *For coherent sequences, nesting implies smallness : $C \cap N \subseteq S$. In other words, if a sequence of* GF(2)*-linear functions $\{h_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ has $h_n(2^i) = h_{n-1}(2^i)$ for $0 \leq i < 2^{n-1}$ and $\mathrm{Tr}_{\alpha_{n-1}}(\breve{h}_n(2^i)) = \mathrm{Tr}_{\alpha_{n-1}}(\breve{h}_n(2^{i+2^{n-1}})) = \breve{h}_{n-1}(2^i)$ for $0 \leq i < 2^{n-1}$, then $h_n(x) \in \mathrm{GF}(\alpha_{n-1})$, for $x \in \mathrm{GF}(\alpha_n)$.*

PROOF. First, since $\breve{h}_n(2^i) \in \mathrm{GF}(\alpha_n)$ for $0 \leq i < 2^n$, we have

$$\begin{aligned} h_n(2^i) &= \sum_{j=1}^{2^n} [f_n]_{i-(-1),j} \breve{h}_n(2^{j-1}) = \sum_{j=1}^{2^n} 2^i \varphi^{j-1} \breve{h}_n(2^{j-1}) \quad \text{(by Equation 3.11)} \\ &< \alpha_n. \end{aligned} \tag{3.44}$$

Since $\{h_n\}$ nests, there exists m such that for all $n \geq m$:

$$\breve{h}_{n+1}(2^i) = \begin{cases} \breve{h}_n(2^i) * \alpha_n + b_i & , 0 \leq i < 2^n; \\ \breve{h}_n(2^{i-2^n}) * \alpha_n + b_i & , 2^n \leq i < 2^{n+1}, \end{cases}$$

for some $b_i \in \mathrm{GF}(\alpha_n)$. Also since $\{h_n\}$ is a coherent sequence, we have $\breve{h}_{n+1}(2^i) + \breve{h}_{n+1}(2^{i+2^n}) = \breve{h}_n(2^i)$, for $0 \leq i < 2^n$ by Theorem 3.44. So

$$b_i + b_{2^n+i} = \breve{h}_n(2^i). \tag{3.45}$$

For $0 \leq i < 2^n$, since $h_{n+1}(2^i) = h_n(2^i)$, and $h_n(2^i) < \alpha_n$ by Equation 3.44, $h_{n+1}(2^i) \in \mathrm{GF}(\alpha_n)$, for $0 \leq i < 2^n$. For $2^n \leq i < 2^{n+1}$, we have $h_{n+1}(2^i)$

$$= \sum_{j=1}^{2^{n+1}} [f_{n+1}]_{i-(-1),j} * \breve{h}_{n+1}(2^j)$$

$$
\begin{aligned}
&= \sum_{j=1}^{2^{n+1}} 2^i \varphi^{j-1} * \breve{h}_{n+1}(2^j) \\
&= \sum_{j=1}^{2^{n+1}} 2^{2^n+(i-2^n)} \varphi^{j-1} * \breve{h}_{n+1}(2^j) \\
&= \sum_{j=1}^{2^{n+1}} (2^{i-2^n} * \alpha_n) \varphi^{j-1} * \breve{h}_{n+1}(2^j) \\
&= \sum_{j=1}^{2^n} (2^{i-2^n} * \alpha_n) \varphi^{j-1} * \breve{h}_{n+1}(2^j) + \sum_{j=2^n}^{2^{n+1}} (2^{i-2^n} * \alpha_n) \varphi^{j-1} * \breve{h}_{n+1}(2^j) \\
&= \sum_{j=1}^{2^n} (2^{i-2^n} * \alpha_n) \varphi^{j-1} * (\breve{h}_n(2^j) * \alpha_n + b_j) \\
&\quad + \sum_{j=2^n}^{2^{n+1}} (2^{i-2^n} * \alpha_n) \varphi^{j-1} * (\breve{h}_n(2^{j-2^n}) * \alpha_n + b_j) \\
&= \sum_{j=1}^{2^n} (2^{i-2^n} * \alpha_n) \varphi^{j-1} * (\breve{h}_n(2^j) * \alpha_n + b_j) \\
&\quad + \sum_{j=1}^{2^n} (2^{i-2^n} * \alpha_n) \varphi^{2^n+(j-1)} * (\breve{h}_n(2^j) * \alpha_n + b_{2^n+j}) \\
&= \sum_{j=1}^{2^n} (2^{i-2^n} * \alpha_n) \varphi^{j-1} * (\breve{h}_n(2^j) * \alpha_n + b_j) \\
&\quad + \sum_{j=1}^{2^n} ((2^{i-2^n} * \alpha_n) \varphi^{2^n}) \varphi^{j-1} * (\breve{h}_n(2^j) * \alpha_n + b_{2^n+j}) \\
&= \sum_{j=1}^{2^n} (2^{i-2^n} * \alpha_n) \varphi^{j-1} * (\breve{h}_n(2^j) * \alpha_n + b_j) \\
&\quad + \sum_{j=1}^{2^n} (2^{i-2^n} * (\alpha_n + 1)) \varphi^{j-1} * (\breve{h}_n(2^j) * \alpha_n + b_{2^n+j}) \\
&= \sum_{j=1}^{2^n} (2^{i-2^n} * \alpha_n) \varphi^{j-1} * \breve{h}_n(2^j) * \alpha_n + \sum_{j=1}^{2^n} (2^{i-2^n} * \alpha_n) \varphi^{j-1} * b_j \\
&\quad + \sum_{j=1}^{2^n} (2^{i-2^n} * \alpha_n) \varphi^{j-1} * \breve{h}_n(2^j) * \alpha_n + \sum_{j=1}^{2^n} 2^{i-2^n} \varphi^{j-1} * \breve{h}_n(2^j) * \alpha_n \\
&\quad + \sum_{j=1}^{2^n} (2^{i-2^n} * \alpha_n) \varphi^{j-1} * b_{2^n+j} + \sum_{j=1}^{2^n} 2^{i-2^n} \varphi^{j-1} * b_{2^n+j}
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{j=1}^{2^n}(2^{i-2^n} * \alpha_n)\varphi^{j-1} * (b_j + b_{2^n+j}) + \sum_{j=1}^{2^n} 2^{i-2^n}\varphi^{j-1} * \breve{h}_n(2^j) * \alpha_n \\
&\quad + \sum_{j=1}^{2^n} 2^{i-2^n}\varphi^{j-1} * b_{2^n+j} \\
&= \sum_{j=1}^{2^n}(2^{i-2^n} * \alpha_n)\varphi^{j-1} * \breve{h}_n(2^j) + \sum_{j=1}^{2^n} 2^{i-2^n}\varphi^{j-1} * \breve{h}_n(2^j) * \alpha_n \\
&\quad + \sum_{j=1}^{2^n} 2^{i-2^n}\varphi^{j-1} * b_{2^n+j} \quad \text{(by (3.45))} \\
&= \sum_{j=1}^{2^n}(2^{i-2^n}\varphi^{j-1} * \alpha_n\varphi^{j-1}) * \breve{h}_n(2^j) + \sum_{j=1}^{2^n} 2^{i-2^n}\varphi^{j-1} * \breve{h}_n(2^j) * \alpha_n \\
&\quad + \sum_{j=1}^{2^n} 2^{i-2^n}\varphi^{j-1} * b_{2^n+j} \\
&= \sum_{j=1}^{2^n}(2^{i-2^n}\varphi^{j-1} * \breve{h}_n(2^j)) * (\alpha_n\varphi^{j-1} + \alpha_n) + \sum_{j=1}^{2^n} 2^{i-2^n}\varphi^{j-1} * b_{2^n+j} \\
&< \alpha_n \quad (\text{since } 2^{i-2^n}\varphi^{j-1},\ \breve{h}_n(2^j),\ \alpha_n\varphi^{j-1} + \alpha_n,\ b_{2^n+j} < \alpha_n).
\end{aligned}
$$

Hence we have $h_{n+1}(2^i) \in \mathrm{GF}(\alpha_n)$, for $x \in \mathrm{GF}(\alpha_{n+1})$. □

Lemma 3.54 $[f_n^{-1}]_{i+2^{n-1},j+2^{n-1}} = [f_n^{-1}]_{i,j+2^{n-1}} = [f_{n-1}^{-1}]_{i,j}$

PROOF. For $1 \le i, j \le 2^{n-1}$,

$$
\begin{aligned}
&[f_n^{-1}]_{i+2^{n-1},j+2^{n-1}} \\
&= P_{2^n-(j+2^{n-1})}\varphi^{i+2^{n-1}-1} \quad \text{(by Corollary 3.35)} \\
&= P_{2^{n-1}-j}\varphi^{i+2^{n-1}-1} \\
&= P_{2^{n-2}+(2^{n-2}-j)}\varphi^{i+2^{n-1}-1} \\
&= (P_{2^{n-2}+(2^{n-2}-j)}\varphi^{2^{n-1}})\varphi^{i-1} \\
&= P_{2^{n-2}+(2^{n-2}-j)}\varphi^{i-1}, \quad \text{since } P_{2^{n-2}+(2^{n-2}-j)} < \alpha_{n-1}, \text{ and by Lemma 3.4} \\
&= P_{2^n-(j+2^{n-1})}\varphi^{i-1}
\end{aligned}
$$

$= [f_n^{-1}]_{i,j+2^{n-1}}$.

Also, since $[f_n^{-1}]_{i,j+2^{n-1}} = P_{2^n-(j+2^{n-1})}\varphi^{i-1} = P_{2^{n-1}-j}\varphi^{i-1} = [f_{n-1}^{-1}]_{i,j}$, we then have $[f_n^{-1}]_{i+2^{n-1},j+2^{n-1}} = [f_n^{-1}]_{i,j+2^{n-1}} = [f_{n-1}^{-1}]_{i,j}$. □

Lemma 3.55 $[f_n^{-1}]_{i,j} < \alpha_n$, *for* $1 \leq i,j \leq 2^n$.

PROOF. By Corollary 3.35, we have $[f_n^{-1}]_{i,j} = P_{2^n-j}\varphi^{i-1}$ for $1 \leq i,j \leq 2^n$. But $P_{2^n-j} < P_{2^n} = \alpha_n + 1$ and $P_{2^n-j} \neq \alpha_n$, so we have $P_{2^n-j} < \alpha_n$, and so $[f_n^{-1}]_{i,j} = P_{2^n-j}\varphi^{i-1} < \alpha_n$, since $\mathrm{GF}(\alpha_n)$ is closed under φ. □

Corollary 3.56 $[f_n^{-1}]_{i,j+2^{n-1}} < \alpha_{n-1}$, *for* $1 \leq i \leq 2^n$ *and* $1 \leq j \leq 2^{n-1}$.

PROOF. Follows by Lemma 3.54 and Lemma 3.55. □

Lemma 3.57 $[f_n^{-1}]_{1,j} = [f_n^{-1}]_{1,j+2^{n-1}} * (\alpha_{n-1}+1)$ *for* $1 \leq j \leq 2^{n-1}$.

PROOF. We know $[f_n^{-1}]_{1,j} = P_{2^n-j}$ and $[f_n^{-1}]_{1,j+2^{n-1}} = P_{2^n-(j+2^{n-1})}$. Now since $1 \leq j \leq 2^{n-1}$, so $2^{n-1} \leq 2^n-j \leq 2^n-1$. Hence the decomposition of 2^n-j as a sum of powers of 2 contains 2^{n-1} for every $1 \leq j \leq 2^{n-1}$. Also, $2^n-j = (2^n-(j+2^{n-1}))+2^{n-1}$. So by Corollary 3.15, $P_{2^n-j} = P_{2^n-(j+2^{n-1})} * P_{2^{n-1}} = P_{2^n-(j+2^{n-1})} * (\alpha_{n-1}+1)$. Hence $[f_n^{-1}]_{1,j} = [f_n^{-1}]_{1,j+2^{n-1}} * (\alpha_{n-1}+1)$. □

Lemma 3.58 *For* $1 \leq i \leq 2^n$ *and* $1 \leq j \leq 2^{n-1}$, $[f_n^{-1}]_{i,j} = [f_n^{-1}]_{i,j+2^{n-1}} * \alpha_{n-1} + C_{n,i,j}$ *for some* $C_{n,i,j} < \alpha_{n-1}$.

PROOF. For $1 \leq i \leq 2^n$ and $1 \leq j \leq 2^{n-1}$,

$[f_n^{-1}]_{i,j} = [f_n^{-1}]_{1,j}\varphi^{i-1}$ (by Corollary 3.35)

$$
\begin{aligned}
&= ([f_n^{-1}]_{1,j+2^{n-1}} * (\alpha_{n-1}+1))\varphi^{i-1} \quad \text{(by Lemma 3.57)} \\
&= ([f_n^{-1}]_{1,j+2^{n-1}} * \alpha_{n-1})\varphi^{i-1} + [f_n^{-1}]_{1,j+2^{n-1}}\varphi^{i-1} \\
&= [f_n^{-1}]_{1,j+2^{n-1}}\varphi^{i-1} * \alpha_{n-1}\varphi^{i-1} + [f_n^{-1}]_{1,j+2^{n-1}}\varphi^{i-1} \\
&= [f_n^{-1}]_{i,j+2^{n-1}} * \alpha_{n-1}\varphi^{i-1} + [f_n^{-1}]_{1,j+2^{n-1}}\varphi^{i-1} \quad \text{(by Corollary 3.35)} \\
&= [f_n^{-1}]_{i,j+2^{n-1}} * (\alpha_{n-1} + \sum_{j=0}^{i-2} \beta_{n-1}\varphi^j) \\
&\quad + [f_n^{-1}]_{1,j+2^{n-1}}\varphi^{i-1} \quad \text{(by Lemma 3.7)} \\
&= [f_n^{-1}]_{i,j+2^{n-1}} * \alpha_{n-1} + [f_n^{-1}]_{i,j+2^{n-1}} * \sum_{j=0}^{i-2} \beta_{n-1}\varphi^j + [f_n^{-1}]_{1,j+2^{n-1}}\varphi^{i-1} \\
&= [f_n^{-1}]_{i,j+2^{n-1}} * \alpha_{n-1} + C_{n,i,j}, \quad \text{for some } C_{n,i,j} < \alpha_{n-1}. \\
&\quad (\text{ since } \sum_{j=0}^{i-2} \beta_{n-1}\varphi^j < \alpha_{n-1} \text{ and } [f_n^{-1}]_{i,j+2^{n-1}},\ [f_n^{-1}]_{i,j+2^{n-1}}\varphi^{i-1} \\
&\quad < \alpha_{n-1} \text{ by Corollary 3.56 and since } \mathrm{GF}(\alpha_n) \text{ is closed under } \varphi).\square
\end{aligned}
$$

Theorem 3.59 *Small, coherent sequences nest : $C \cap S \subseteq N$. In other words, if a sequence of* GF(2)*-linear functions* $\{h_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ *ultimately has* $h_n(x) \in \mathrm{GF}(\alpha_{n-1})$, *for* $x \in \mathrm{GF}(\alpha_n)$ *and* $h_n(2^i) = h_{n-1}(2^i)$, *for* $0 \le i < 2^{n-1}$, *then* $\mathrm{Tr}_{\alpha_{n-1}}(\breve{h}_n(2^i)) = \mathrm{Tr}_{\alpha_{n-1}}(\breve{h}_n(2^{i+2^{n-1}}))$
$= \breve{h}_{n-1}(2^i)$ for $0 \le i < 2^{n-1}$.

PROOF. For $1 \le i \le 2^{n-1}$,

$$
\begin{aligned}
\breve{h}_n(2^i) &= \sum_{j=1}^{2^n} [f_n^{-1}]_{i,j} * h_n(2^{j-1}) \\
&= \sum_{j=1}^{2^{n-1}} [f_n^{-1}]_{i,j} * h_n(2^{j-1}) + \sum_{j=2^{n-1}+1}^{2^n} [f_n^{-1}]_{i,j} * h_n(2^{j-1}) \\
&= \sum_{j=1}^{2^{n-1}} ([f_n^{-1}]_{i,j+2^{n-1}} * \alpha_{n-1} + C_{n,i,j}) * h_n(2^{j-1}) + \sum_{j=2^{n-1}+1}^{2^n} [f_n^{-1}]_{i,j} * h_n(2^{j-1}) \\
&\quad (\text{ for some } C_{n,i,j} < \alpha_{n-1}, \text{ by Lemma 3.58})
\end{aligned}
$$

$$= \sum_{j=1}^{2^{n-1}} [f_n^{-1}]_{i,j+2^{n-1}} * \alpha_{n-1} * h_n(2^{j-1}) + \sum_{j=1}^{2^{n-1}} C_{n,i,j} * h_n(2^{j-1}) + \sum_{j=2^{n-1}+1}^{2^n} [f_n^{-1}]_{i,j} * h_n(2^{j-1}).$$

Now since $C_{n,i,j} < \alpha_{n-1}$, $h_n(2^{j-1}) < \alpha_{n-1}$ by smallness, and $[f_n^{-1}]_{i,j} < \alpha_{n-1}$ for $1 \leq i \leq 2^n, 2^{n-1}+1 \leq j \leq 2^n$ by Corollary 3.56. Thus for some $C_i < \alpha_{n-1}$, one has

$$\begin{aligned}
\breve{h}_n(2^i) &= (\sum_{j=1}^{2^{n-1}} [f_n^{-1}]_{i,j+2^{n-1}} * h_n(2^{j-1})) * \alpha_{n-1} + C_i \\
&= (\sum_{j=1}^{2^{n-1}} [f_{n-1}^{-1}]_{i,j} * h_n(2^{j-1})) * \alpha_{n-1} + C_i \quad \text{(by Lemma 3.4)} \\
&= (\sum_{j=1}^{2^{n-1}} [f_{n-1}^{-1}]_{i,j} * h_{n-1}(2^{j-1})) * \alpha_{n-1} + C_i \quad \text{(by hypothesis)} \\
&= \breve{h}_{n-1}(2^i) * \alpha_{n-1} + C_i.
\end{aligned}$$

So we have $\mathrm{Tr}_{\alpha_{n-1}}(\breve{h}_n(2^i)) = \breve{h}_{n-1}(2^i)$. Also,

$$\begin{aligned}
\breve{h}_n(2^{i+2^{n-1}}) &= \sum_{j=1}^{2^n} [f_n^{-1}]_{i+2^{n-1},j} * h_n(2^{j-1}) \\
&= \sum_{j=1}^{2^{n-1}} [f_n^{-1}]_{i+2^{n-1},j} * h_n(2^{j-1}) + \sum_{j=2^{n-1}+1}^{2^n} [f_n^{-1}]_{i+2^{n-1},j} * h_n(2^{j-1}) \\
&= \sum_{j=1}^{2^{n-1}} ([f_n^{-1}]_{i+2^{n-1},j+2^{n-1}} * \alpha_{n-1} + C_{n,i+2^{n-1},j}) * h_n(2^{j-1}) + \\
&\quad \sum_{j=2^{n-1}+1}^{2^n} [f_n^{-1}]_{i+2^{n-1},j} * h_n(2^{j-1}) \quad \text{(for some } C_{n,i+2^{n-1},j} < \alpha_{n-1}, \\
&\quad \text{by Lemma 3.58)} \\
&= \sum_{j=1}^{2^{n-1}} [f_n^{-1}]_{i+2^{n-1},j+2^{n-1}} * \alpha_{n-1} * h_n(2^{j-1}) + \sum_{j=1}^{2^{n-1}} C_{n,i+2^{n-1},j} * h_n(2^{j-1}) \\
&\quad + \sum_{j=2^{n-1}+1}^{2^n} [f_n^{-1}]_{i+2^{n-1},j} * h_n(2^{j-1}).
\end{aligned}$$

Now since $C_{n,i+2^{n-1},j} < \alpha_{n-1}$, $h_n(2^{j-1}) < \alpha_{n-1}$ by smallness, and $[f_n^{-1}]_{i+2^{n-1},j} < \alpha_{n-1}$ for $1 \leq i \leq 2^n$, we have $2^{n-1}+1 \leq j \leq 2^n$ by Corollary 3.56. Thus for some

$C_i < \alpha_{n-1}$,

$$\begin{aligned}
\breve{h}_n(2^i) &= (\sum_{j=1}^{2^{n-1}} [f_n^{-1}]_{i+2^{n-1},j+2^{n-1}} * h_n(2^{j-1})) * \alpha_{n-1} + C_i \\
&= (\sum_{j=1}^{2^{n-1}} [f_{n-1}^{-1}]_{i,j} * h_n(2^{j-1})) * \alpha_{n-1} + C_i \quad \text{(by Lemma 3.4)} \\
&= (\sum_{j=1}^{2^{n-1}} [f_{n-1}^{-1}]_{i,j} * h_{n-1}(2^{j-1})) * \alpha_{n-1} + C_i \quad \text{(by hypothesis)} \\
&= \breve{h}_{n-1}(2^i) * \alpha_{n-1} + C_i.
\end{aligned}$$

So $\mathrm{Tr}_{\alpha_{n-1}}(\breve{h}_n(2^{i+2^{n-1}})) = \breve{h}_{n-1}(2^i)$, i.e. $\{h_n\}$ nests. □

Corollary 3.60 *For coherent sequences, the concepts of nesting and smallness coincide. Thus* $C \cap N = C \cap S$.□

Lemma 3.61 $\mathrm{Tr}_{\alpha_{n-1}}(P_{2^n-i}\varphi^j) = P_{2^{n-1}-i}\varphi^j$ for $1 \le i \le 2^{n-1}$.

PROOF. By Corollary 3.14, we have $P_{2^n-i}\varphi^j = P_{2^{n-1}-i}\varphi^j * \alpha_{n-1} + P_{2^{n-1}-i} * \sum_{k=0}^{j-1} \beta_{n-1}\varphi^k +$ $P_{2^{n-1}-i}\varphi^j$ *for* $1 \le i \le 2^{n-1}$. So $\mathrm{Tr}_{\alpha_{n-1}}(P_{2^n-i}\varphi^j) = P_{2^{n-1}-i}\varphi^j$, since $P_{2^{n-1}-i} * \sum_{k=0}^{j-1} \beta_{n-1}\varphi^k + P_{2^{n-1}-i}\varphi^j < \alpha_{n-1}$. □

Lemma 3.62 *For small sequences, nesting implies coherence :* $S \cap N \subseteq C$. *In other words, if a sequence of* GF(2)*-linear functions* $\{h_n : \mathrm{GF}(\alpha_n) \to \mathrm{GF}(\alpha_n)\}$ *ultimately has* $h_n(x) \in \mathrm{GF}(\alpha_{n-1})$, *for* $x \in \mathrm{GF}(\alpha_n)$ *and* $\mathrm{Tr}_{\alpha_{n-1}}(\breve{h}_n(2^i)) = \mathrm{Tr}_{\alpha_{n-1}}(\breve{h}_n(2^{i+2^{n-1}})) = \breve{h}_{n-1}(2^i)$ for $0 \le i < 2^{n-1}$, then $h_n(2^i) = h_{n-1}(2^i)$, for $0 \le i < 2^{n-1}$.

PROOF. First we denote $h_{n-1}(2^i)$ by a_i, and $h_n(2^i)$ by b_i, for $0 \le i < 2^{n-1}$. Since $\{h_n\}$ is a small sequence, we have $a_i,\ b_i < \alpha_{n-1}$, for $0 \le i < 2^{n-1}$. we want to show $a_i = b_i$, for $0 \le i < 2^{n-1}$. Since $\{h_n\}$ is a nesting sequence, we have

$$\mathrm{Tr}_{\alpha_{n-1}}(\breve{h}_n(2^i)) = \breve{h}_{n-1}(2^i), \tag{3.46}$$

for $0 \leq i < 2^{n-1}$. Now by Corollary 3.35, $\breve{h}_{n-1}(2^i) = \sum_{j=1}^{2^{n-1}} [f_{n-1}^{-1}]_{i-(-1),j} * h_{n-1}(2^{j-1}) = \sum_{j=1}^{2^{n-1}} P_{2^{n-1}-j}\varphi^i * h_{n-1}(2^{j-1}) = \sum_{j=1}^{2^{n-1}} a_{j-1} * P_{2^{n-1}-j}\varphi^i$ and $\breve{h}_n(2^i) = \sum_{j=1}^{2^{n-1}} [f_n^{-1}]_{i-(-1),j} * h_{n-1}(2^{j-1}) = \sum_{j=1}^{2^n} P_{2^n-j}\varphi^i * h_n(2^{j-1}) = \sum_{j=1}^{2^n} b_{j-1} * P_{2^n-j}\varphi^i$. So, $\mathrm{Tr}_{\alpha_{n-1}}(\breve{h}_n(2^i))$

$$
\begin{aligned}
&= \mathrm{Tr}_{\alpha_{n-1}}\Big(\sum_{j=1}^{2^n} b_{j-1} * P_{2^n-j}\varphi^i\Big) \\
&= \mathrm{Tr}_{\alpha_{n-1}}\Big(\sum_{j=1}^{2^{n-1}} b_{j-1} * P_{2^n-j}\varphi^i\Big), \text{ since } P_{2^n-j}\varphi^i < \alpha_{n-1}, \text{ for } 2^{n-1} < j \leq 2^n \\
&\quad \text{and } b_{j-1} < \alpha_{n-1}, \text{ so } b_{j-1} * P_{2^n-j}\varphi^i < \alpha_{n-1}, \text{ for } 2^{n-1} < j \leq 2^n. \\
&= \sum_{j=1}^{2^{n-1}} b_{j-1} * \mathrm{Tr}_{\alpha_{n-1}}(P_{2^n-j}\varphi^i) \\
&= \sum_{j=1}^{2^{n-1}} b_{j-1} * (P_{2^{n-1}-j}\varphi^i) \quad (\text{ by Lemma 3.61})
\end{aligned}
$$

By Equation 3.46, we then have $\sum_{j=1}^{2^{n-1}} a_{j-1} * P_{2^{n-1}-j}\varphi^i = \sum_{j=1}^{2^{n-1}} b_{j-1} * P_{2^{n-1}-j}\varphi^i$, for $0 \leq i < 2^{n-1}$. i.e. $\sum_{j=1}^{2^{n-1}} (a_{j-1} + b_{j-1}) * P_{2^{n-1}-j}\varphi^i = 0.$, for $0 \leq i < 2^{n-1}$. i.e.

$$
\begin{bmatrix}
P_{2^{n-1}-1} & P_{2^{n-1}-2} & \cdots & P_0 \\
P_{2^{n-1}-1}\varphi & P_{2^{n-1}-2}\varphi & \cdots & P_0\varphi \\
\vdots & \vdots & \cdots & \vdots \\
P_{2^{n-1}-1}\varphi^{2^{n-1}-1} & P_{2^{n-1}-2}\varphi^{2^{n-1}-1} & \cdots & P_0\varphi^{2^{n-1}-1}
\end{bmatrix}
\begin{bmatrix}
a_0 + b_0 \\
a_1 + b_1 \\
\vdots \\
a_{2^{n-1}-1} + b_{2^{n-1}-1}
\end{bmatrix}
= 0.
$$

Notice that the $2^{n-1} \times 2^{n-1}$matrix on the left hand side of the equality is f_{n-1}^{-1}. We know the $\det(f_{n-1}) = 1$ by Lemma 3.18, so $\det(f_{n-1}^{-1}) = 1$ too. Since the determine is not equal to 0, the equation above has unique solution which is the 0 vector. i.e. $a_i = b_i$, for $0 \leq i < 2^{n-1}$. So we proved $\{h_n\}$ is a coherent sequence. □

Corollary 3.63 $C \cap N = N \cap S = S \cap C$.□

References

[Co] J.H.Conway, *On Numbers and Games*, Camb. Univ. Press, Cambridge, 1975.

[Co2] J. H. Conway, *Integral lexicographic codes*, Discrete Mathematics 83 (1990), 219-235.

[HHS] F.-L. Hsu, F.A. Hummer and J.D.H. Smith, *Logarithms, syndrome functions, and the information rates of greedy loop transversal codes*, Journal of Combinatorial Mathematics and Combinatorial Computing (to appear).

[HmS] F.A. Hummer and J.D.H. Smith, *Greedy loop transversal codes,metrics, and lexicodes,* Journal of Combinatorial Mathematics and Combinatorial Computing (to appear).

[Le] H. W. Lenstra, Jr., *Nim multiplication*, Séminaire de Théorie des Nombres . (1977-78), 11-01 – 11-23.

[Le2] H. W. Lenstra, Jr., Solution to Problem 566, Nieuw Archief voor Wiskunde 28(1980), 300-302.

[Sm] J.D.H. Smith, *Loop transversals to linear codes*, J. Comb., Info. and Syst. Sci. **17** (1992), 1-8.

Table 3.1: The 16 × 16 transform matrix f_4

FFFF	5555	3333	1111	0F0F	0505	0303	0101	FF	55	33	11	F	5	3	1
9CAF	785A	2EE48	19C4	0959	07F7	02C2	0181	9C	78	2E	19	9	7	2	1
CD64	46B8	3C41	1482	0C13	0421	03FA	015F	CD	46	3C	14	C	4	3	1
B380	6240	2750	1EF0	0B8A	0645	025B	01F6	B3	62	27	1E	B	6	2	1
F0F2	5053	3034	1018	0FF0	0550	0330	0110	F0	50	30	10	F	5	3	1
95F5	7FAF	2C8C	1848	09C5	078F	02EC	0198	95	7F	2C	18	9	7	2	1
C175	429A	3FBE	15D7	0CDE	0467	03C6	014B	C1	42	3F	15	C	4	3	1
B809	6407	250C	1F08	0B39	0627	027C	01E8	B8	64	25	1F	B	6	2	1
FF00	5500	3300	1100	0F00	0500	0300	0100	FF	55	33	11	F	5	3	1
9C33	7822	2E66	19DD	0950	07F0	02C0	0180	9C	78	2E	19	9	7	2	1
CDA9	46FE	3C7D	1496	0C1F	0425	03F9	015E	CD	46	3C	14	C	4	3	1
B333	6222	2777	1EEE	0B81	0643	0259	01F7	B3	62	27	1E	B	6	2	1
F002	5003	3004	1008	0FFF	0555	0333	0111	F0	50	30	10	F	5	3	1
9560	7FD0	2CA0	1850	09CC	0788	02EE	0199	95	7F	2C	18	9	7	2	1
C1B4	42D8	3F81	15C2	0CD2	0463	03C5	014A	C1	42	3F	15	C	4	3	1
B8B1	6463	2529	1F17	0B32	0621	027E	01E9	B8	64	25	1F	B	6	2	1

Table 3.2: The first row of f_4 as Pascal's Triangle modulo 2

							1								
						1		1							
					1		0		1						
				1		1		1		1					
			1		0		0		0		1				
		1		1		0		0		1		1			
	1		0		1		0		1		0		1		
1		1		1		1		1		1		1		1	
	1		0		0		0		0		0		0		1
		1		1		0		0		0		0		1	1
	1		0		1		0		0		0		1		0	1
		1		1		1		1		0		0		0		0		1		1		1		1
	1		0		0		0		1		0		0		0		1		0		0		0		1
		1		1		0		0		1		1		0		0		1		1		0		0		1		1
	1		0		1		0		1		0		1		0		1		0		1		0		1		0		1
1		1		1		1		1		1		1		1		1		1		1		1		1		1		1		1

CHAPTER 4. EXPONENTIATION IN THE QUADRATIC CLOSURE OF GF(2)

Theorem 4.6 below represents a key result on exponentiation in the quadratic closure of GF(2). It was originally proved by H. W. Lenstra, Jr. in 1980 [Le2]. In this chapter, we give an alternative, more elementary approach to the proof of this result. First, it is convenient to establish some special notation. Set:

$$\begin{aligned} S_n &= \sum_{0\le i<j<2^n} \beta_n\varphi^i * \beta_n\varphi^j \\ &= \sum_{i=1}^{2^n-1} (\beta_n\varphi^i * \sum_{j=0}^{i-1} \beta_n\varphi^j) \\ &= \sum_{i=0}^{2^n-2} (\beta_n\varphi^i * \sum_{j=i+1}^{2^n-1} \beta_n\varphi^j); \end{aligned} \tag{4.1}$$

$$T_n = \sum_{i=0}^{2^{n-1}-2} (\beta_n\varphi^i * \sum_{j=i+1}^{2^{n-1}-1} \beta_n\varphi^j); \tag{4.2}$$

$$D_n = \sum_{i=0}^{2^n-1} (\beta_n * \beta_{n+1})\varphi^i; \tag{4.3}$$

$$E_n = \sum_{i=0}^{2^n-1} (\beta_n * \beta_n\varphi)\varphi^i. \tag{4.4}$$

Lemma 4.1 *$x\varphi^{2^n} = x + a$, where $x = a * \alpha_n + b$, $0 \le a, b < \alpha_n$.*

PROOF.

$$\begin{aligned} x\varphi^{2^n} &= (a * \alpha_n + b)\varphi^{2^n} \\ &= a\varphi^{2^n} * \alpha_n\varphi^{2^n} + b\varphi^{2^n} \\ &= a * (\alpha_n + 1) + b, \text{ since } 0 \leq a, b < \alpha_n \\ &= a * \alpha_n + a + b \\ &= a * \alpha_n + b + a \\ &= x + a.\square \end{aligned}$$

Lemma 4.2 $\beta_n\varphi^{2^{n-1}} = \beta_n^{\alpha_{n-1}} = \beta_n + \beta_{n-1}$.

PROOF.

$$\begin{aligned} \beta_n\varphi^{2^{n-1}} &= (\beta_{n-1} * \alpha_{n-1})\varphi^{2^{n-1}} \\ &= \beta_{n-1}\varphi^{2^{n-1}} * \alpha_{n-1}\varphi^{2^{n-1}} \\ &= \beta_{n-1} * (1 + \alpha_{n-1}), \text{ by Lemma 3.4 and Lemma 3.8} \\ &= \beta_{n-1} + \beta_{n-1} * \alpha_{n-1} \\ &= \beta_{n-1} + \beta_n, \text{ by Lemma 3.6.}\square \end{aligned}$$

Lemma 4.3 *If* $a \in \mathrm{GF}(\alpha_{n-1})$, *then* $a\varphi^{2^{n-i}} = a\varphi^{2^{n-1-i}}$.

PROOF. $a\varphi^{2^{n-i}} = a\varphi^{2^{n-1}-(-2^{n-1})-i} = a\varphi^{2^{n-1}+(2^{n-1}-i)} = (a\varphi^{2^{n-1}})\varphi^{(2^{n-1}-i)}$
$= a\varphi^{2^{n-1}-i}$, by Lemma 3.4.$\square$

Lemma 4.4 $\beta_n\varphi^k \geq \beta_n$, *for all* n, $k \geq 0$

PROOF. We will prove the lemma by induction on n.

(Base) We have $\beta_0 = 1$, and $\beta_0\varphi^k = 1$ for all $k \geq 0$, so $\beta_0\varphi^k \geq \beta_0$.

(IH) Assume $\forall k$, $\beta_n\varphi^k \geq \beta_n$

(IS)

$$\begin{aligned}
\beta_{n+1}\varphi^k &= (\alpha_n * \beta_n)\varphi^k, \text{ by Lemma 3.6} \\
&= \alpha_n\varphi^k * \beta_n\varphi^k \\
&= (\alpha_n + \sum_{i=0}^{k-1} \beta_n\varphi^i) * \beta_n\varphi^k, \text{ by Lemma 3.7} \\
&= \beta_n\varphi^k * \alpha_n + (\sum_{i=0}^{k-1} \beta_n\varphi^i) * \beta_n\varphi^k. \\
&\geq \beta_n * \alpha_n, \quad \text{since } \beta_n\varphi^k, (\sum_{i=0}^{k-1} \beta_n\varphi^i) * \beta\varphi^k < \alpha_n, \text{ and by (IH).} \\
&= \beta_{n+1}, \text{ by Lemma 3.6.}\square
\end{aligned}$$

Lemma 4.5

If $\beta_n * \beta_n\varphi > \beta_n$, *then* $\beta_{n+1} * \beta_{n+1}\varphi < \beta_{n+1}$.

If $\beta_n * \beta_n\varphi < \beta_n$, *then* $\beta_{n+1} * \beta_{n+1}\varphi > \beta_{n+1}$.

PROOF.

$$\begin{aligned}
\beta_{n+1} * \beta_{n+1}\varphi &= (\alpha_n * \beta_n) * (\alpha_n * \beta_n)\varphi \\
&= \alpha_n * \beta_n * \alpha_n\varphi * \beta_n\varphi \\
&= \alpha_n * \beta_n * (\alpha_n + \beta_n) * \beta_n\varphi \\
&= \alpha_n * \beta_n * \alpha_n * \beta_n\varphi + \alpha_n * \beta_n * \beta_n * \beta_n\varphi
\end{aligned}$$

$$
\begin{aligned}
&= \alpha_n^2 * \beta_n * \beta_n\varphi + \alpha_n * \beta_n * \beta_n * \beta_n\varphi \\
&= (\alpha_n + \beta_n) * \beta_n * \beta_n\varphi + \alpha_n * \beta_n * \beta_n * \beta_n\varphi \\
&= \alpha_n * (\beta_n * \beta_n\varphi + \beta_n * \beta_n * \beta_n\varphi) + \beta_n * \beta_n * \beta_n\varphi \\
&= \alpha_n * (\beta_n * \beta_n\varphi + \beta_n\varphi^2) + \beta_n\varphi^2.
\end{aligned}
$$

By Lemma 4.4, $\beta_n\varphi^2 \geq \beta_n$. So if $\beta_n * \beta_n\varphi > \beta_n$, then $\beta_n * \beta_n\varphi + \beta_n\varphi^2 < \beta_n$, so $\beta_{n+1} * \beta_{n+1}\varphi < \alpha_n * \beta_n = \beta_{n+1}$, while if $\beta_n * \beta_n\varphi < \beta_n$, then $\beta_n * \beta_n\varphi + \beta_n\varphi^2 > \beta_n$, so $\beta_{n+1} * \beta_{n+1}\varphi > \alpha_n * \beta_n = \beta_{n+1}$.□

Corollary 4.6

$$\beta_n * \beta_n\varphi > \beta_n, \quad \textit{when } n \textit{ is even.}$$

$$\beta_n * \beta_n\varphi < \beta_n, \quad \textit{when } n \textit{ is odd.}$$

PROOF. $\beta_1 * \beta_1\varphi = 2 * 3 = 1 < 2 = \beta_1$.

The rest follows by induction using Lemma 4.5. □

Lemma 4.7 $D_n = \alpha_n + E_n + S_n + \beta_n$.

PROOF. $D_n = \sum_{i=0}^{2^n-1} (\beta_n * \beta_{n+1})\varphi^i$

$= \sum_{i=0}^{2^n-1} (\beta_n * \alpha_n * \beta_n)\varphi^i$, by Lemma 3.6

$= \sum_{i=0}^{2^n-1} (\alpha_n * \beta_n\varphi)\varphi^i$

$= \sum_{i=0}^{2^n-1} \alpha_n\varphi^i * \beta_n\varphi^{i+1}$

$= \alpha_n * \beta_n\varphi + \sum_{i=1}^{2^n-1} (\alpha_n\varphi^i * \beta_n\varphi^{i+1})$

$$= \alpha_n * \beta_n\varphi + \sum_{i=1}^{2^n-1}(\alpha_n + \sum_{j=0}^{i-1}\beta_n\varphi^j) * \beta_n\varphi^{i+1}$$

$$= \alpha_n * \beta_n\varphi + \sum_{i=1}^{2^n-1}\alpha_n * \beta_n\varphi^{i+1} + \sum_{i=1}^{2^n-1}(\sum_{j=0}^{i-1}\beta_n\varphi^j * \beta_n\varphi^{i+1})$$

$$= \alpha_n * (\beta_n\varphi + \sum_{i=1}^{2^n-1}\beta_n\varphi^{i+1}) + \sum_{i=1}^{2^n-1}(\sum_{j=0}^{i-1}\beta_n\varphi^j * \beta_n\varphi^{i+1})$$

$$= \alpha_n * \sum_{i=0}^{2^n-1}\beta_n\varphi^{i+1} + \sum_{i=1}^{2^n-2}(\sum_{j=0}^{i-1}\beta_n\varphi^j * \beta_n\varphi^{i+1}) + (\sum_{j=0}^{2^n-2}\beta_n\varphi^j) * \beta_n\varphi^{2^n}$$

$$= \alpha_n * (\sum_{i=0}^{2^n-1}\beta_n\varphi^i)\varphi + \sum_{i=1}^{2^n-2}[(\beta_n\varphi^i + \sum_{j=0}^{i}\beta_n\varphi^j) * \beta_n\varphi^{i+1}]$$

$+(1 + \beta_n\varphi^{2^n-1}) * \beta_n\varphi^{2^n}$, by Lemma 3.10

$$= \alpha_n * 1\varphi + \sum_{i=1}^{2^n-2}(\beta_n\varphi^i * \beta_n\varphi^{i+1}) + \sum_{i=1}^{2^n-2}(\sum_{j=0}^{i}\beta_n\varphi^j * \beta_n\varphi^{i+1}) + \beta_n\varphi^{2^n}$$

$+\beta_n\varphi^{2^n} * \beta_n\varphi^{2^n-1}$, by Lemma 3.10

$$= \alpha_n + \sum_{i=1}^{2^n-2}(\beta_n\varphi^i * \beta_n\varphi^{i+1}) + \sum_{i=2}^{2^n-1}(\sum_{j=0}^{i-1}\beta_n\varphi^j * \beta_n\varphi^i) + \beta_n + \beta_n\varphi^{2^n} * \beta_n\varphi^{2^n-1},$$

by Lemma 3.4 and change of indices

$$= \alpha_n + \sum_{i=1}^{2^n-2}(\beta_n\varphi^i * \beta_n\varphi^{i+1}) + \sum_{i=1}^{2^n-1}\sum_{j=0}^{i-1}(\beta_n\varphi^j * \beta_n\varphi^i) + \beta_n * \beta_n\varphi + \beta_n$$

$+\beta_n\varphi^{2^n} * \beta_n\varphi^{2^n-1}$

$$= \alpha_n + \sum_{i=1}^{2^n-2}(\beta_n\varphi^i * \beta_n\varphi^{i+1}) + \beta_n\varphi^{2^n} * \beta_n\varphi^{2^n-1} + \sum_{i=1}^{2^n-1}(\sum_{j=0}^{i-1}\beta_n\varphi^j) * \beta_n\varphi^i$$

$+\beta_n * \beta_n\varphi + \beta_n$

$$= \alpha_n + \sum_{i=1}^{2^n-1}(\beta_n\varphi^i * \beta_n\varphi^{i+1}) + (S_n + \beta_n * \beta_n\varphi) + \beta_n$$

$$= \alpha_n + \sum_{i=1}^{2^n-1}(\beta_n\varphi^i * \beta_n\varphi^{i+1} + \beta_n * \beta_n\varphi) + S_n + \beta_n$$

$$= \alpha_n + \sum_{i=0}^{2^n-1}(\beta_n\varphi^i * \beta_n\varphi^{i+1}) + S_n + \beta_n$$

$$= \alpha_n + \sum_{i=0}^{2^n-1}(\beta_n * \beta_n\varphi)\varphi^i + S_n + \beta_n$$

$= \alpha_n + E_n + S_n + \beta_n$, by (4.4). □

Corollary 4.8

If n is even and $S_n = 0$, *then* $D_n = \alpha_n + \beta_n + 1$.

If n is even and $S_n = 1$, *then* $D_n = \alpha_n + \beta_n$.

If n is odd and $S_n = 0$, *then* $D_n = \alpha_n + \beta_n$.

If n is odd and $S_n = 1$, *then* $D_n = \alpha_n + \beta_n + 1$.

PROOF. If n is even, we have $\beta_n * \beta_n\varphi > \beta_n$ by Corollary 4.6. So $E_n = \sum_{i=0}^{2^n-1} (\beta_n * \beta_n\varphi)\varphi^i$ $= 1$ by Lemma 3.10. If n is odd, we have $\beta_n * \beta_n\varphi < \beta_n$ by Corollary 4.6. So $E_n = \sum_{i=0}^{2^n-1} (\beta_n * \beta_n\varphi)\varphi^i = 0$ by Lemma 3.9. The results follow by Lemma 4.7. □

Lemma 4.9 $\sum_{i=0}^{2^n-1} \beta_{n+1}\varphi^i = \alpha_n + S_n$.

PROOF.

$$\begin{aligned}
\sum_{i=0}^{2^n-1} \beta_{n+1}\varphi^i &= \sum_{i=0}^{2^n-1} (\alpha_n * \beta_n)\varphi^i, \text{ by Lemma 3.6} \\
&= \alpha_n * \beta_n + \sum_{i=1}^{2^n-1} \alpha_n\varphi^i * \beta_n\varphi^i \\
&= \alpha_n * \beta_n + \sum_{i=1}^{2^n-1} \beta_n\varphi^i * (\alpha_n + \sum_{j=0}^{i-1} \beta_n\varphi^j), \text{ by Lemma 3.7} \\
&= \alpha_n * \beta_n + \sum_{i=1}^{2^n-1} \beta_n\varphi^i * \alpha_n + \sum_{i=1}^{2^n-1} (\beta_n\varphi^i * \sum_{j=0}^{i-1} \beta_n\varphi^j) \\
&= \sum_{i=0}^{2^n-1} \beta_n\varphi^i * \alpha_n + S_n, \text{ by (4.2)} \\
&= \alpha_n + S_n, \text{ by Lemma 3.10.□}
\end{aligned}$$

Lemma 4.10 $\alpha_{n+1}^{\alpha_n} = \alpha_{n+1} + \alpha_n + S_n$.

PROOF.

$\alpha_{n+1}^{\alpha_n} = \alpha_{n+1}\varphi^{2^n} = \alpha_{n+1} + \sum_{i=0}^{2^n-1} \beta_{n+1}\varphi^i$, by Lemma 3.7

$= \alpha^{n+1} + \alpha_n + S_n$, by Lemma 4.9. □

Lemma 4.11 *$\alpha_n^{\alpha_{n-1}} = \alpha_n\varphi^{2^{n-1}} = \alpha_n + \alpha_{n-1} + k_n$, where $k_n = 0$ or 1.*

PROOF.

$$\begin{aligned} \alpha_n^{\alpha_{n-1}} &= \alpha_n + \sum_{i=0}^{2^{n-1}-1} \beta_n\varphi^i \\ &= \alpha_n + \alpha_{n-1} + (\alpha_{n-1} + \sum_{i=0}^{2^{n-1}-1} \beta_n\varphi^i), \text{ by Lemma 3.7.} \end{aligned}$$

Let $k_n = \alpha_{n-1} + \sum_{i=0}^{2^{n-1}-1} \beta_n\varphi^i$. We have $\alpha_n^{\alpha_{n-1}} = \alpha_n + \alpha_{n-1} + k_n$,

and

$$\begin{aligned} k_n\varphi &= \alpha_{n-1}\varphi + \sum_{i=0}^{2^{n-1}-1} \beta_n\varphi^{i+1} \\ &= \alpha_{n-1} + \beta_{n-1} + \sum_{i=1}^{2^{n-1}} \beta_n\varphi^i, \text{ by Lemma 3.7 and change of indices.} \end{aligned}$$

So

$$\begin{aligned} k_n + k_n\varphi &= \alpha_{n-1} + \sum_{i=0}^{2^{n-1}-1} \beta_n\varphi^i + \alpha_{n-1} + \beta_{n-1} + \sum_{i=1}^{2^{n-1}} \beta_n\varphi^i \\ &= (\beta_n + \sum_{i=1}^{2^{n-1}-1} \beta_n\varphi^i) + \beta_{n-1} + (\sum_{i=1}^{2^{n-1}-1} \beta_n\varphi^i + \beta_n\varphi^{2^{n-1}}) \\ &= \beta_n + \beta_{n-1} + \beta_n\varphi^{2^{n-1}} \\ &= \beta_n + \beta_{n-1} + \beta_n + \beta_{n-1}, \text{ by Lemma 4.2} \\ &= 0 \quad . \end{aligned}$$

Since $0 = k_n + k_n\varphi = k_n + k_n^2 = k_n(1 + k_n)$, we have $k_n = 0$ or $k_n = 1$,

i.e. $\alpha_n^{\alpha_{n-1}} = \alpha^n + \alpha_{n-1} + k_n$, where $k_n = 0$ or 1.□

Lemma 4.12 $\sum_{i=0}^{2^{n-1}-1} \beta_n\varphi^i * (\sum_{i=0}^{2^{n-1}-1} \beta_n\varphi^i)\varphi^{2^{n-1}} = \beta_{n-1}$.

PROOF.

From Lemma 4.11 and Lemma 3.7, we have $\sum_{i=0}^{2^{n-1}-1} \beta_n\varphi^i = \alpha_{n-1} + k_n$, where $k_n = 0$ or 1.

Also, since $k_n = 0$ or 1, so $k_n\varphi^m = k_n$, for all m. (*)

So

$$\begin{aligned}
&\sum_{i=0}^{2^{n-1}-1} \beta_n\varphi^i * (\sum_{i=0}^{2^{n-1}-1} \beta_n\varphi^i)\varphi^{2^{n-1}} \\
&= (\alpha_{n-1} + k_n) * (\alpha_{n-1} + k_n)\varphi^{2^{n-1}} \\
&= (\alpha_{n-1} + k_n) * (\alpha_{n-1}\varphi^{2^{n-1}} + k_n\varphi^{2^{n-1}}) \\
&= (\alpha_{n-1} + k_n) * ((\alpha_{n-1} + 1) + k_n), \text{ by Lemma 3.8 and (*)} \\
&= \alpha_{n-1}^2 + k_n\alpha_{n-1} + \alpha_{n-1} + k_n + k_n\alpha_{n-1} + k_n^2 \\
&= \alpha_{n-1}^2 + \alpha_{n-1} + k_n + k_n, \text{ by (*)} \\
&= (\alpha_{n-1} + \beta_{n-1}) + \alpha_{n-1}, \text{ by Lemma 3.7} \\
&= \beta_{n-1}.\square
\end{aligned}$$

Lemma 4.13 $T_n + T_n\varphi^{2^{n-1}} = \alpha_{n-1} + D_{n-1}$.

PROOF. $T_n\varphi^{2^{n-1}}$

$$\begin{aligned}
&= \sum_{i=0}^{2^{n-1}-2} (\beta_n\varphi^i * \sum_{j=i+1}^{2^{n-1}-1} \beta_n\varphi^j)\varphi^{2^{n-1}} \\
&= \sum_{i=0}^{2^{n-1}-2} (\beta_n\varphi^{i+2^{n-1}} * \sum_{j=i+1}^{2^{n-1}-1} \beta_n\varphi^{j+2^{n-1}}) \\
&= \sum_{i=0}^{2^{n-1}-2} [(\beta_n\varphi^{2^{n-1}})\varphi^i * \sum_{j=i+1}^{2^{n-1}-1} (\beta_n\varphi^{2^{n-1}})\varphi^j]
\end{aligned}$$

$$= \sum_{i=0}^{2^{n-1}-2} [(\beta_n + \beta_{n-1})\varphi^i * \sum_{j=i+1}^{2^{n-1}-1} (\beta_n + \beta_{n-1})\varphi^j], \text{ by Lemma 4.2}$$

$$= \sum_{i=0}^{2^{n-1}-2} [(\beta_n\varphi^i + \beta_{n-1}\varphi^i) * \sum_{j=i+1}^{2^{n-1}-1} (\beta_n\varphi^j + \beta_{n-1}\varphi^j)]$$

$$= \sum_{i=0}^{2^{n-1}-2} (\beta_n\varphi^i * \sum_{j=i+1}^{2^{n-1}-1} \beta_n\varphi^j) + \sum_{i=0}^{2^{n-1}-2} (\beta_n\varphi^i * \sum_{j=i+1}^{2^{n-1}-1} \beta_{n-1}\varphi^j)$$

$$+ \sum_{i=0}^{2^{n-1}-2} (\beta_{n-1}\varphi^i * \sum_{j=i+1}^{2^{n-1}-1} \beta_n\varphi^j) + \sum_{i=0}^{2^{n-1}-2} (\beta_{n-1}\varphi^i * \sum_{j=i+1}^{2^{n-1}-1} \beta_{n-1}\varphi^j)$$

$$= T_n + \sum_{i=0}^{2^{n-1}-2} (\beta_n\varphi^i * \sum_{j=i+1}^{2^{n-1}-1} \beta_{n-1}\varphi^j) + \sum_{i=1}^{2^{n-1}-1} (\beta_n\varphi^i * \sum_{j=0}^{i-1} \beta_{n-1}\varphi^j) + S_{n-1}$$

$$= T_n + [\beta_n * \sum_{j=1}^{2^{n-1}-1} \beta_{n-1}\varphi^j + \sum_{i=1}^{2^{n-1}-2} (\beta_n\varphi^i * \sum_{j=i+1}^{2^{n-1}-1} \beta_{n-1}\varphi^j)]$$

$$+ [\sum_{i=1}^{2^{n-1}-2} (\beta_n\varphi^i * \sum_{j=0}^{i-1} \beta_{n-1}\varphi^j) + \beta_n\varphi^{2^{n-1}-1} * \sum_{j=0}^{2^{n-1}-2} \beta_{n-1}\varphi^j] + S_{n-1}$$

$$= T_n + \beta_n * \sum_{j=1}^{2^{n-1}-1} \beta_{n-1}\varphi^j + \sum_{i=1}^{2^{n-1}-2} [\beta_n\varphi^i * (\sum_{j=i+1}^{2^{n-1}-1} \beta_{n-1}\varphi^j + \sum_{j=0}^{i-1} \beta_{n-1}\varphi^j)]$$

$$+ \beta_n\varphi^{2^{n-1}-1} * \sum_{j=0}^{2^{n-1}-2} \beta_{n-1}\varphi^j + S_{n-1}$$

$$= T_n + \beta_n * (\beta_{n-1} + \sum_{j=0}^{2^{n-1}-1} \beta_{n-1}\varphi^j) + \sum_{i=1}^{2^{n-1}-2} [\beta_n\varphi^i * (\beta_{n-1}\varphi^i + \sum_{j=0}^{2^{n-1}-1} \beta_{n-1}\varphi^j)]$$

$$+ \beta_n\varphi^{2^{n-1}-1} * (\sum_{j=0}^{2^{n-1}-1} \beta_{n-1}\varphi^j + \beta_{n-1}\varphi^{2^{n-1}-1}) + S_{n-1}$$

$$= T_n + \beta_n * (\beta_{n-1} + 1) + \sum_{i=1}^{2^{n-1}-2} [\beta_n\varphi^i * (\beta_{n-1}\varphi^i + 1)] + \beta_n\varphi^{2^{n-1}-1} * (1 + \beta_{n-1}\varphi^{2^{n-1}-1}) + S_{n-1},$$

by Lemma 3.10

$$= T_n + \sum_{i=0}^{2^{n-1}-1} [\beta_n\varphi^i * (1 + \beta_{n-1}\varphi^i)] + S_{n-1}$$

$$= T_n + \sum_{i=0}^{2^{n-1}-1} \beta_n\varphi^i + \sum_{i=0}^{2^{n-1}-1} \beta_n\varphi^i * \beta_{n-1}\varphi^i + S_{n-1}$$

$$= T_n + (\alpha_{n-1} + S_{n-1}) + D_{n-1} + S_{n-1}, \text{ by Lemma 4.9 and (4.3)}$$

$$= T_n + \alpha_{n-1} + D_{n-1}.$$

So $T_n + T_n\varphi^{2^{n-1}} = \alpha_{n-1} + D_{n-1}$.□

Lemma 4.14 $S_n = \beta_{n-1} + \alpha_{n-1} + D_{n-1}$.

PROOF. $S_n = \sum_{i=0}^{2^n-2} (\beta_n\varphi^i * \sum_{j=i+1}^{2^n-1} \beta_n\varphi^j)$

$= \sum_{i=0}^{2^{n-1}-1} (\beta_n\varphi^i * \sum_{j=i+1}^{2^n-1} \beta_n\varphi^j) + \sum_{i=2^{n-1}}^{2^n-2} (\beta_n\varphi^i * \sum_{j=i+1}^{2^n-1} \beta_n\varphi^j).$

$= \sum_{i=0}^{2^{n-1}-1} [\beta_n\varphi^i * (\sum_{j=i+1}^{2^{n-1}-1} \beta_n\varphi^j + \sum_{j=2^{n-1}}^{2^n-1} \beta_n\varphi^j)] + \sum_{i=0}^{2^{n-1}-2} (\beta_n\varphi^{i+2^{n-1}} * \sum_{j=i+2^{n-1}+1}^{2^n-1} \beta_n\varphi^j)$

$= \sum_{i=0}^{2^{n-1}-2} (\beta_n\varphi^i * \sum_{j=i+1}^{2^{n-1}-1} \beta_n\varphi^j) + \sum_{i=0}^{2^{n-1}-1} (\beta_n\varphi^i * \sum_{j=2^{n-1}}^{2^n-1} \beta_n\varphi^j)$

$+ \sum_{i=0}^{2^{n-1}-2} (\beta_n\varphi^{i+2^{n-1}} * \sum_{j=i+1}^{2^{n-1}-1} \beta_n\varphi^{j+2^{n-1}})$

$= \sum_{i=0}^{2^{n-1}-2} (\beta_n\varphi^i * \sum_{j=i+1}^{2^{n-1}-1} \beta_n\varphi^j) + \sum_{i=0}^{2^{n-1}-1} (\beta_n\varphi^i * \sum_{j=0}^{2^{n-1}-1} \beta_n\varphi^{j+2^{n-1}})$

$+ [\sum_{i=0}^{2^{n-1}-2} (\beta_n\varphi^i * \sum_{j=i+1}^{2^{n-1}-1} \beta_n\varphi^j)]\varphi^{2^{n-1}}$

$= T_n + (\sum_{i=0}^{2^{n-1}-1} \beta_n\varphi^i) * (\sum_{j=0}^{2^{n-1}-1} \beta_n\varphi^j)\varphi^{2^{n-1}} + T_n\varphi^{2^{n-1}}$, by (4.2)

$= T_n + T_n\varphi^{2^{n-1}} + (\sum_{i=0}^{2^{n-1}-1} \beta_n\varphi^i) * (\sum_{j=0}^{2^{n-1}-1} \beta_n\varphi^j)\varphi^{2^{n-1}}$

$= \alpha_{n-1} + D_{n-1} + \beta_{n-1}$, by Lemma 4.13 and Lemma 4.12. □

Lemma 4.15 *Let $n = 4r + k$, where $r \geq 0$ and $0 \leq k < 4$. Then we have:*

$$S_n = 0, \quad \textit{when } k = 0 \textit{ or } 3;$$

$$S_n = 1, \quad \textit{when } k = 1 \textit{ or } 2. \tag{4.5}$$

PROOF. We will prove the lemma by induction on r.

(Base) From Lemma 8, we have $\alpha_{n+1}^{\alpha_n} = \alpha_{n+1} + \alpha_n + S_n$. Now

$\alpha_1^{\alpha_0} = \alpha_1 + \alpha_0$, so $S_0 = 0$;

$\alpha_2^{\alpha_1} = \alpha_2 + \alpha_1 + 1$, so $S_1 = 1$;

$\alpha_3^{\alpha_2} = \alpha_3 + \alpha_2 + 1$, so $S_2 = 1$;

$\alpha_4^{\alpha_3} \doteq \alpha_4 + \alpha_3$, so $S_3 = 0$.

(IH) Assume (4.5) is true for $r \leq t$ and $0 \leq k < 4$.

(IS) We want to show (3.7) is true for $r = t+1$ and $0 \leq k < 4$ too.

(1) $r = t+1, k = 0$: then $n = 4(t+1)+0 = 4t+4$, and $n-1 = 4t+3$.

By (IH), we have $S_{n-1} = S_{4t+3} = 0$.

Since $n-1 = 4t+3$ is an odd number, we have $D_{n-1} = \alpha_{n-1} + \beta_{n-1}$ by Corollary 4.5.

Now by Lemma 4.14, we have

$$\begin{aligned} Sn &= S_{4t+4} = \beta_{n-1} + \alpha_{n-1} + D_{n-1} \\ &= \beta_{n-1} + \alpha_{n-1} + (\alpha_{n-1} + \beta_{n-1}) \\ &= 0. \end{aligned}$$

(2) $r = t+1, k = 1$: then $n = 4(t+1)+1 = 4t+5$, and $n-1 = 4t+4$.

By (1), we have $S_{n-1} = S_{4t+4} = 0$.

Since $n-1 = 4t+4$ is an even number, we have $D_{n-1} = \alpha_{n-1} + \beta_{n-1} + 1$ by Corollary 4.5.

Now by Lemma 4.14, we have

$$\begin{aligned} Sn &= S_{4t+5} = \beta_{n-1} + \alpha_{n-1} + D_{n-1} \\ &= \beta_{n-1} + \alpha_{n-1} + (\alpha_{n-1} + \beta_{n-1} + 1) \\ &= 1. \end{aligned}$$

(3) $r = t+1, k = 2$: then $n = 4(t+1)+2 = 4t+6$, and $n-1 = 4t+5$.

By (2), we have $S_{n-1} = S_{4t+5} = 1$.

Since $n-1 = 4t+5$ is an odd number, we have $D_{n-1} = \alpha_{n-1}+\beta_{n-1}+1$ by Corollary 4.5.

Now by Lemma 4.14, we have

$$\begin{aligned} Sn &= S_{4t+6} = \beta_{n-1} + \alpha_{n-1} + D_{n-1} \\ &= \beta_{n-1} + \alpha_{n-1} + (\alpha_{n-1} + \beta_{n-1} + 1) \\ &= 1. \end{aligned}$$

(4) $r = t+1, k = 3$: then $n = 4(t+1)+3 = 4t+7$, and $n-1 = 4t+6$.

By (3), we have $S_{n-1} = S_{4t+6} = 1$.

Since $n-1 = 4t+6$ is an even number, we have $D_{n-1} = \alpha_{n-1}+\beta_{n-1}$ by Corollary 4.5.

Now by Lemma 4.14, we have

$$\begin{aligned} Sn &= S_{4t+7} = \beta_{n-1} + \alpha_{n-1} + D_{n-1} \\ &= \beta_{n-1} + \alpha_{n-1} + (\alpha_{n-1} + \beta_{n-1}) \\ &= 0. \end{aligned}$$

So we showed that (4.5) is true for $r = t+1$ and $0 \le k < 4$. □

Theorem 4.16 *Let $n = 4r + k$, where $r \ge 0$, and $0 \le k < 4$. Then we have:*

$$\alpha_{n+1}^{\alpha_n} = \alpha_{n+1} + \alpha_n, \quad \textit{when } k = 0 \textit{ or } 3;$$

$$\alpha_{n+1}^{\alpha_n} = \alpha_{n+1} + \alpha_n + 1, \quad \textit{when } k = 1 \textit{ or } 2.$$

PROOF. By Lemma 4.10 and Lemma 4.15. □

CHAPTER 5. CONCLUSION

The loop transversal method is a new approach to the design of linear error-correcting block codes. In the binary case, greedy loop transversal codes coincide with the Conway/Sloane lexicodes. However, in a good channel, the greedy loop transversal method provides a more efficient way of constructing these codes. It has been used to determine the dimensions of the codes for channel lengths up to the sixties (and three hundreds for double errors). In the ternary case, loop transversal codes are not lexicodes. The greedy loop transversal method is being used in an attempt to construct "record breaking" codes.

The graphs of the syndrome functions of the loop transversal codes in the binary case have curious fractal properties. The syndrome functions may be interpreted as polynomials in Conway's field $\mathbf{On}_2$. Passing from such a polynomial function to its coefficient sequence provides a linear transform, analogous to the discrete Fourier transform. Despite the sizes of the transform matrices, we are able to construct the inverse matrices. Also, some interesting properties inherent in the field $\mathbf{On}_2$ are discussed.

The inverse transformation matrices F_{2^n} obtained in Chapter 3 may be used to derive the transforms, i.e. the coefficient sequences, of the greedy white-noise binary syndromes presented in Chapter 2. Figures 5.1 - 5.4 display the 32-dimensional

transforms of the t-error syndromes, for $1 \leq t \leq 4$. Figure 5.5 displays the 256-dimensional transform of the 2-error syndrome. Two features are readily apparent from these transforms. The first is the apparent simplicity of the transforms when compared with the original syndromes. The second is the similarity of the transforms for the various values of t. This similarity illustrates the way in which the syndrome functions generalize the logarithm function.

Future topics include the investigation of methods for the construction of linear codes in modules over rings and corresponding non-linear binary codes.

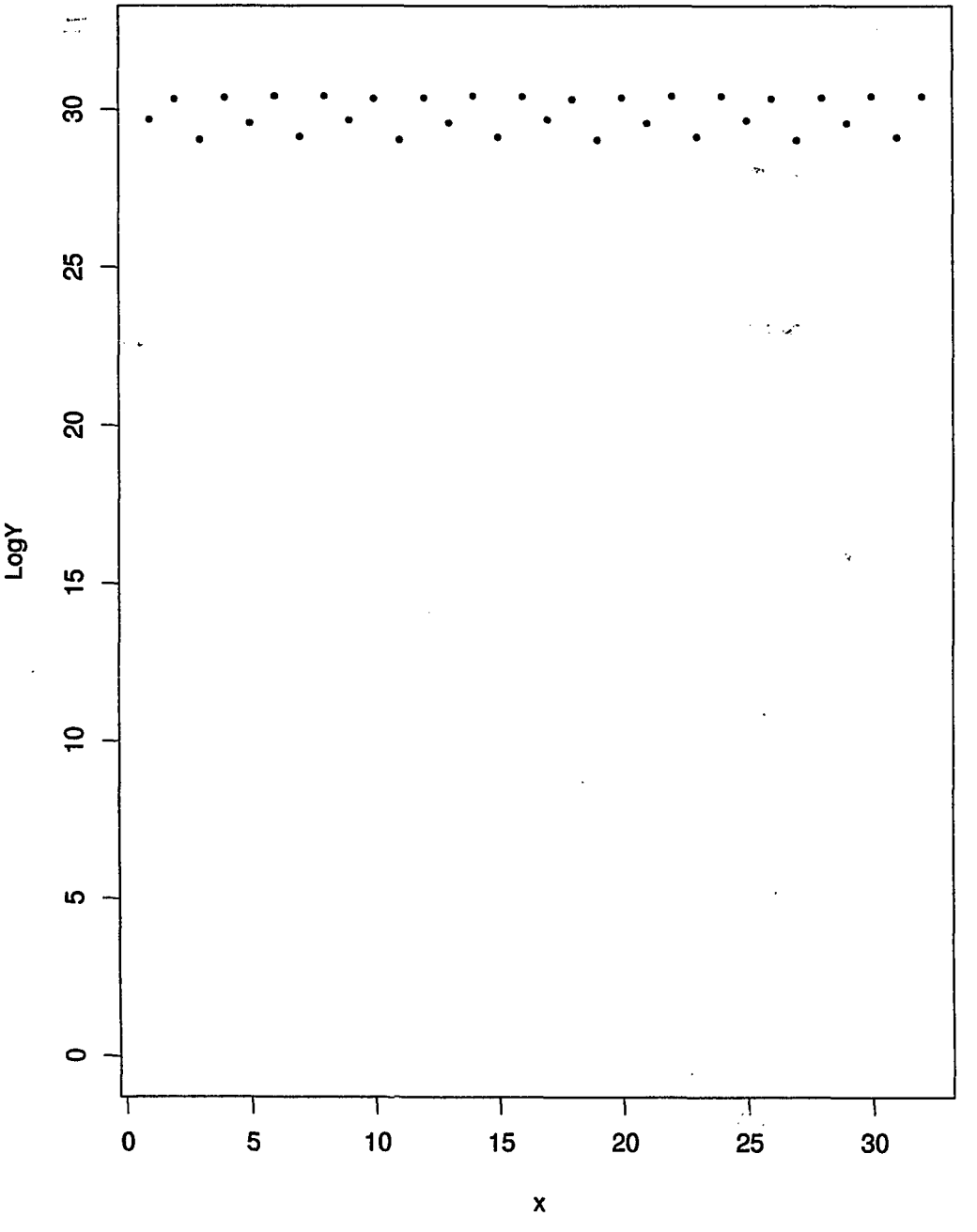

Figure 5.1: Transformed syndrome function (n=32, t=1)

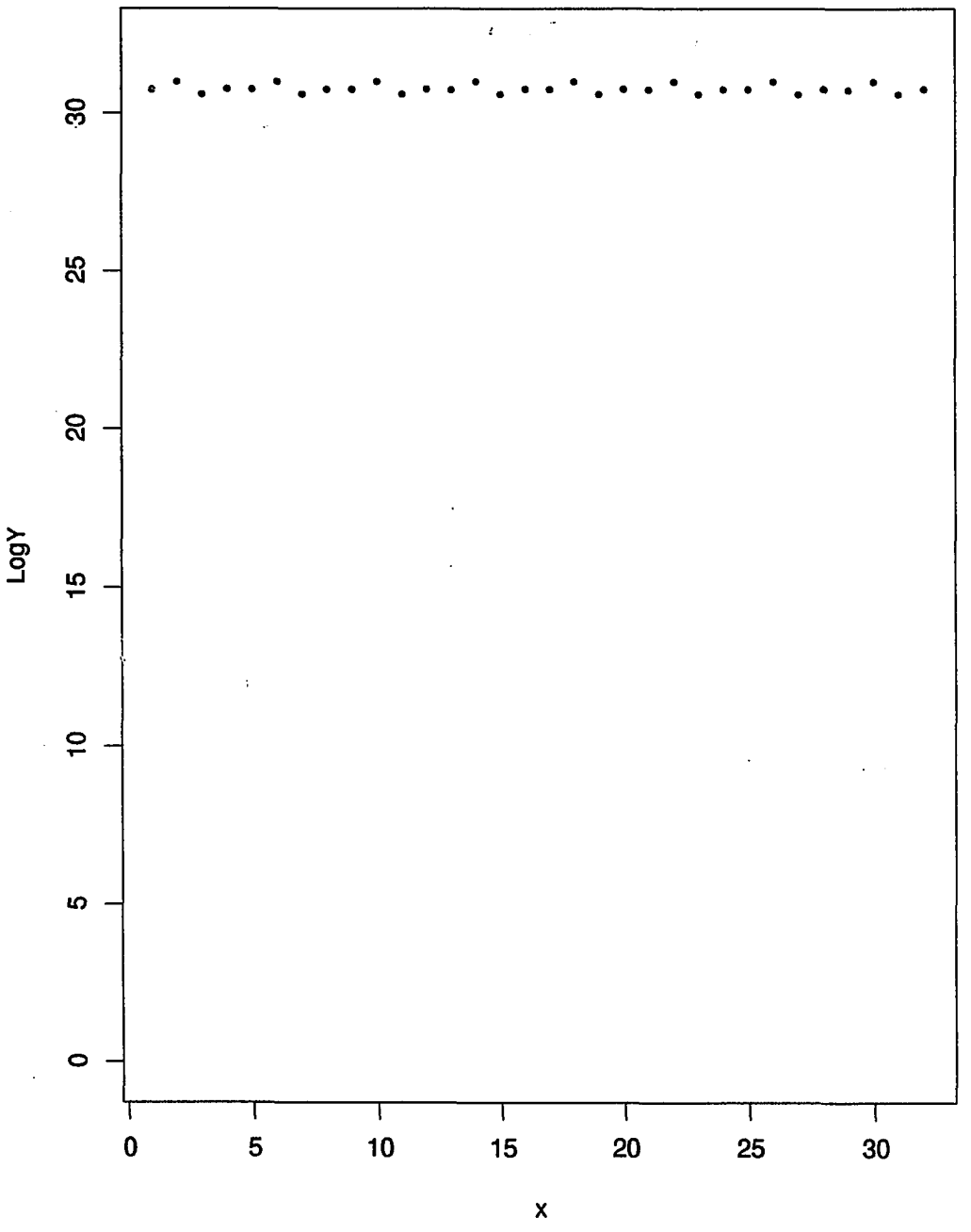

Figure 5.2: Transformed syndrome function (n=32, t=2)

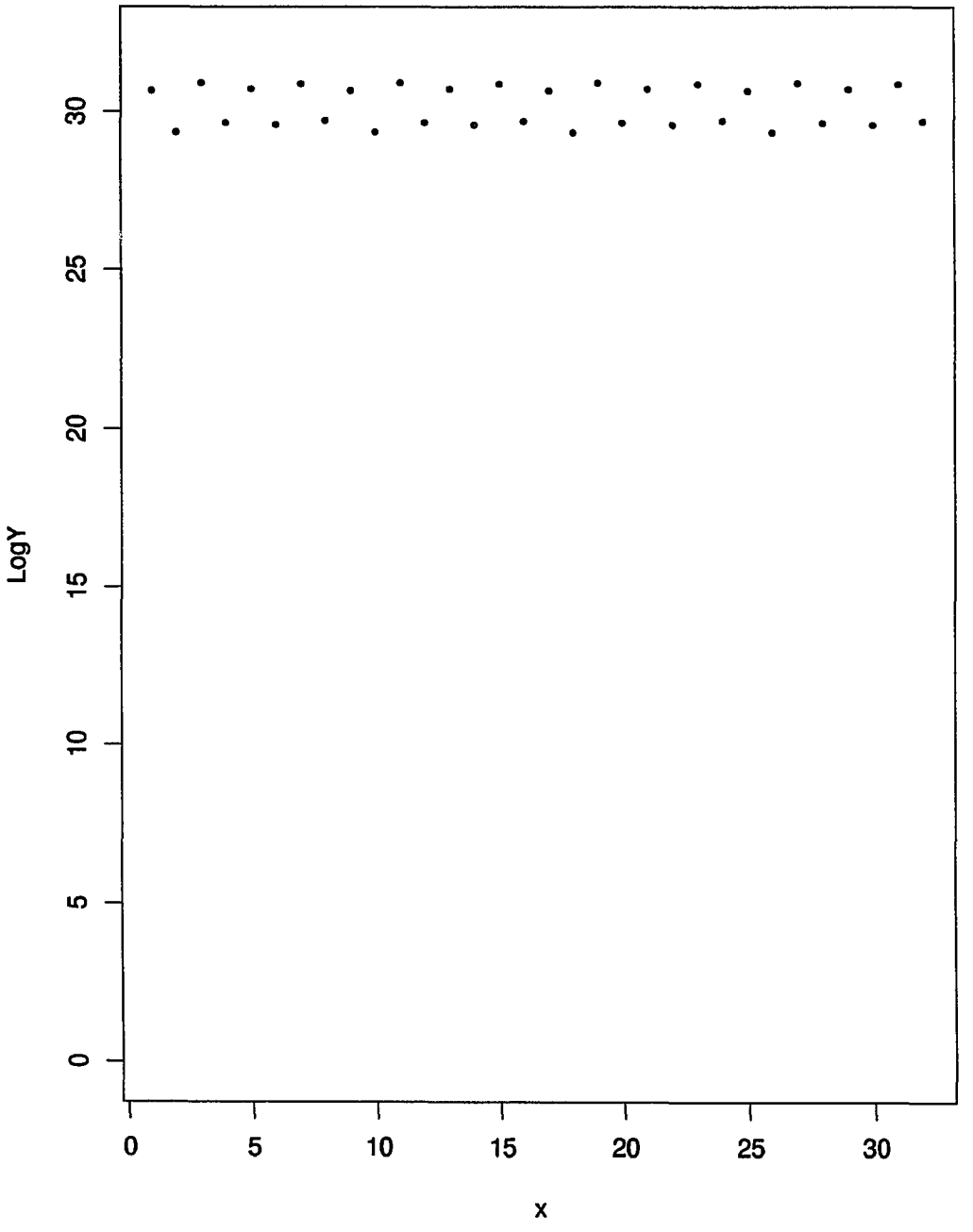

Figure 5.3: Transformed syndrome function (n=32, t=3)

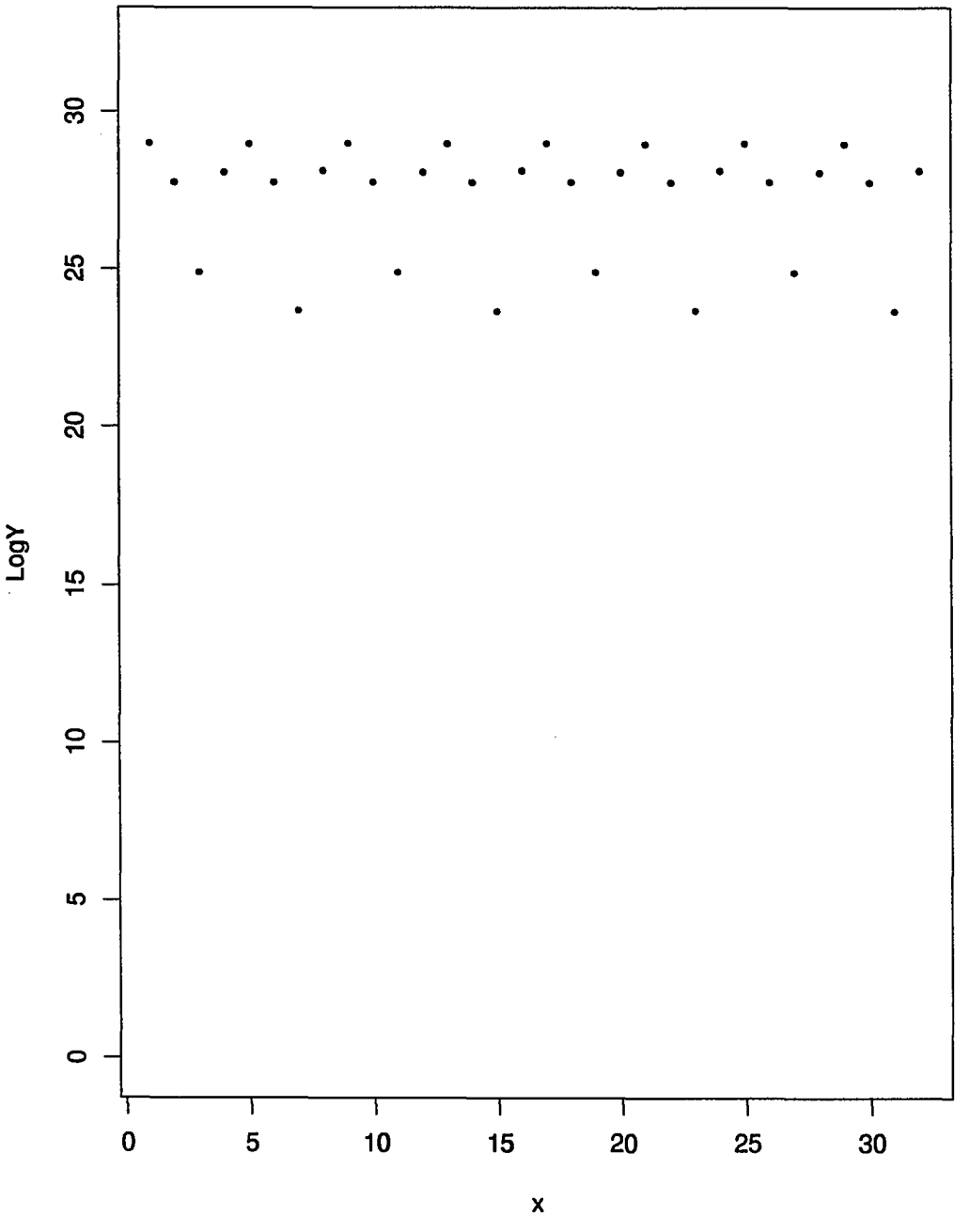

Figure 5.4: Transformed syndrome function (n=32, t=4)

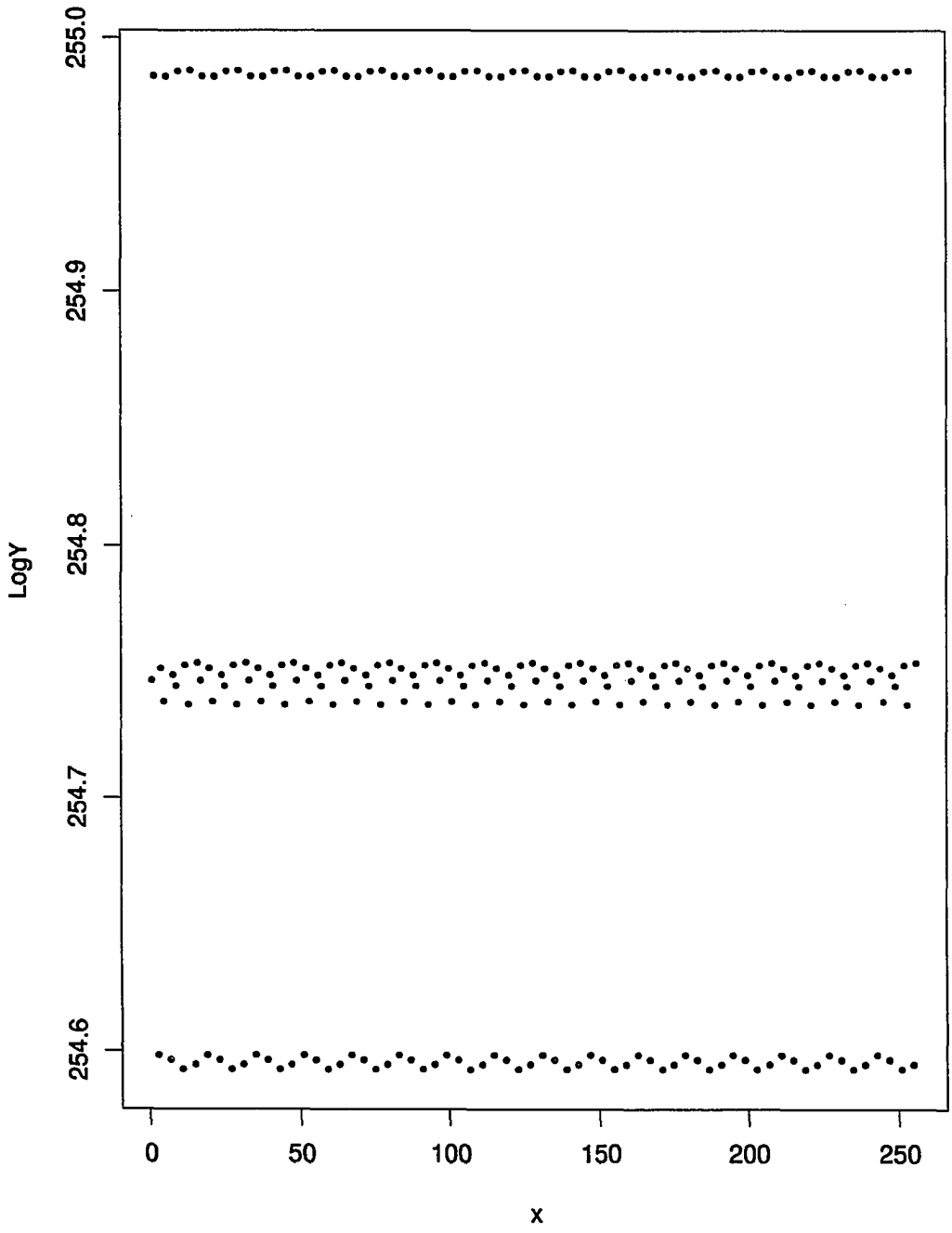

Figure 5.5: Transformed syndrome function (n=256, t=2)

BIBLIOGRAPHY

[Co] J.H.Conway, *On Numbers and Games*, Camb. Univ. Press, Cambridge, 1975.

[Co2] J. H. Conway, *Integral lexicographic codes*, Discrete Mathematics 83 (1990), 219-235.

[HHS] F.-L. Hsu, F.A. Hummer and J.D.H. Smith, *Logarithms, syndrome functions, and the information rates of greedy loop transversal codes*, Journal of Combinatorial Mathematics and Combinatorial Computing (to appear).

[HmS] F.A. Hummer and J.D.H. Smith, *Greedy loop transversal codes,metrics, and lexicodes,* Journal of Combinatorial Mathematics and Combinatorial Computing (to appear).

[KP] F.R. Kschischang and S. Pasupathy,*Some ternary and quaternary codes and associated sphere packings*,I.E.E.E. Trans. Info. Th. **IT-38**,(1992), 227–246.

[Le] H. W. Lenstra, Jr., *Nim multiplication*, Séminaire de Théorie des Nombres (1977-78), 11-01 – 11-23.

[Le2] H. W. Lenstra, Jr., Solution to Problem 566, Nieuw Archief voor Wiskunde 28(1980), 300-302.

[Sm] J.D.H. Smith, *Loop transversals to linear codes*, J. Comb., Info. and Syst. Sci. **17** (1992), 1-8.

[Ve] T. Verhoeff *An updated table of minimum-distance bounds for binary linear codes*, I.E.E.E. Trans. Info. Th. **IT-33** (1987), 665–680